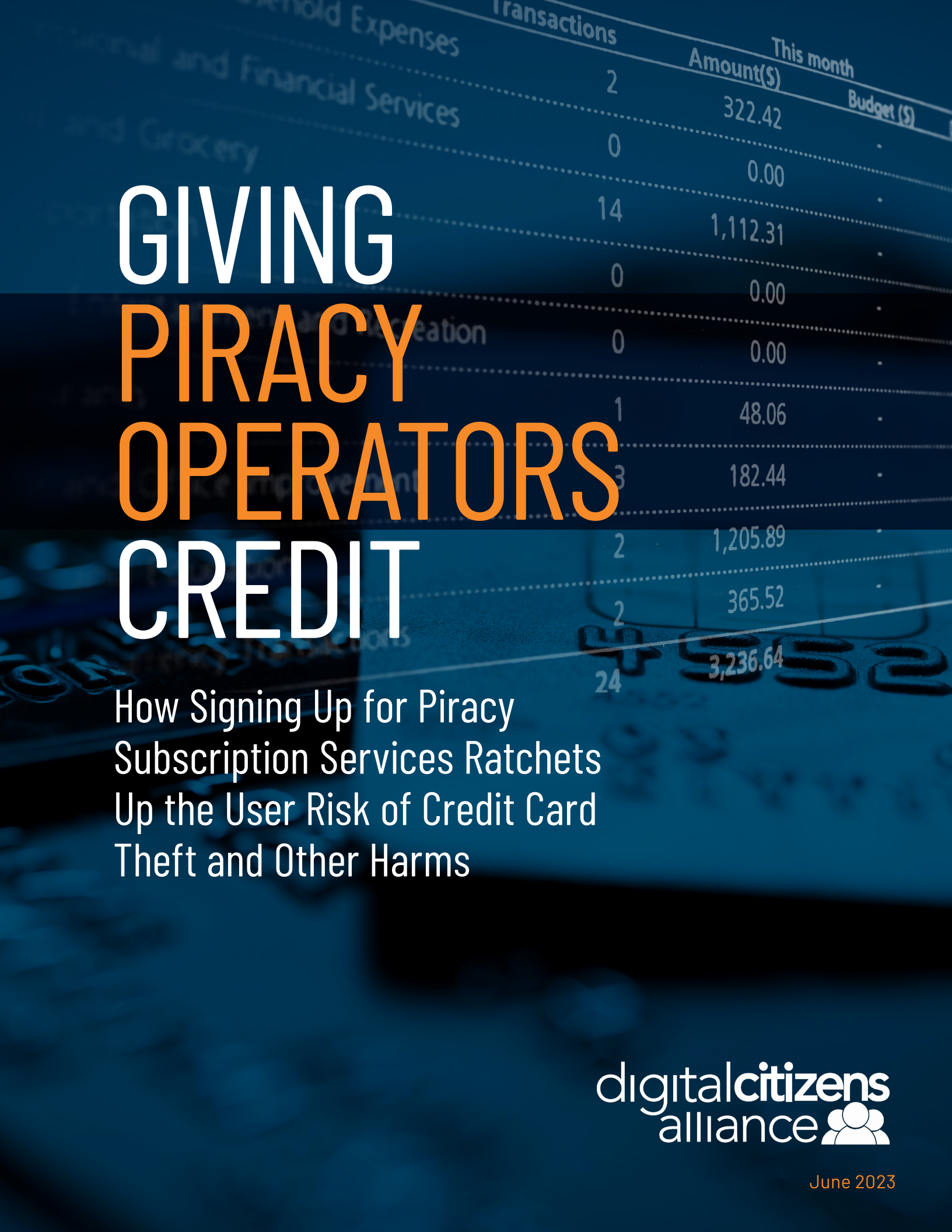

GIVING PIRACY OPERATORS CREDIT

How Signing Up for Piracy Subscription Services Ratchets Up the User Risk of Credit Card Theft and Other Harms

digitalcitizens alliance

June 2023

Table of Contents

Executive Summary

Internet users that use a credit card to sign up for illegal piracy streaming services to gain access to movies, TV shows, and games face a serious risk of having their card run up with charges they didn't authorize, according to a new Digital Citizens Alliance investigation.

Within weeks of signing up for piracy subscription services, Digital Citizens investigators' credit card was targeted for $1,495 in illicit purchases – purportedly for grocery delivery, women's apparel, computer software, a cash advance, and a large mystery charge of $850 that, fortunately, wasn't processed. These purchases appear to originate from China, Singapore, Hong Kong, and Lithuania.

The investigation also conducted survey research that found that the investigators' experience was not isolated. According to the survey of 2,330 Americans, Internet users who signed up for a piracy subscription service using a credit card were 4 times more likely to report unwanted credit card purchases than those who said they don't visit piracy websites and apps. In all, a whopping 72 percent of those who used a credit card to sign up for a piracy service reported credit card fraud.

These revelations add to a growing concern that piracy operators give unwitting users more than they bargained for. In recent years, piracy has been closely linked to the spread of dangerous malware. Last year, Digital Citizens released a video that showed a ransomware attack on investigators visiting piracy websites. The attacker encrypted computer files. Criminals then demanded payment to unlock them. This specific cyber threat was observed across multiple piracy sites.

These findings underscore that while piracy was once primarily a headache for content creators, users of these sites now face significant risks. Piracy subscription services make an estimated $1 billion a year providing services to at least nine million U.S. households.

In their ruthless thirst for greater profit, the illicit actors appear to be more than willing to abuse the trust of unsuspecting users who hand over their credit card information in hopes of getting access to pirated movies and TV shows.

In doing so, these illicit actors are helping fuel an explosion of credit card and other identity theft-related crimes. According to the Federal Trade Commission, Americans lost $5.8 billion from such fraud in 2021, the last year for which there is confirmed data. That fraud was more than double what occurred in 2020.

When confronted with a credit card breach, most Americans have only a vague suspicion about where the exposure may have originated. With this new research, it's common sense to conclude that handing over credit card information to a piracy operator leaves users vulnerable to financial fraud.

And these findings also underscore why a greater collective effort must be taken to protect Internet users. Those efforts should include:

- Payment processors terminating relationships with known piracy operators.
- The FTC making it a priority of warning Americans about online risks that can expose them to financial fraud and malware.
- Law enforcement using the tools they were given in 2020 to launch criminal investigations against piracy operators.
- Consumer protection groups must warn Americans about the risks.

Bad actors rely upon unsuspecting Internet users to trick and steal from them. Often, the user is embarrassed or views fraud as an unavoidable cost of using the Internet. That shouldn't be accepted. Through awareness, diligent law enforcement, and cutting off piracy operators' ability to use and abuse credit card systems, Internet users can take back control of their digital world.

Giving Piracy Operators Credit

Piracy, the theft of movies, TV shows, and games, didn't become a $2 billion industry without adapting. And, in recent years, these illicit actors have re-invented themselves as consumers shifted to streaming content. So, just like Netflix, Disney+, Hulu, and other legitimate providers, piracy operators now offer subscription services to access a world of stolen content.

To sign up, a user simply provides a credit card or other means of payment. In exchange for a fee, subscribers are promised access to pirated content. They get it – and more. Digital Citizens initiated the investigation based on anecdotal reports that users who signed up were prone to be victimized.

To test whether credit card fraud was tied to piracy subscription services, Digital Citizens signed up for twenty piracy subscription services using a new Capital One QuickSilver credit card that was used solely for this project.

From February through April, researchers used the card to sign up for twenty piracy subscription services that accepted credit cards. The full list is below:

Iview HD (iviewhdtv.com)	MOM IPTV (momiptv.shop)
PolBox (polbox.tv)	BayouBengalTV (bayoubengaltv.us/1)
Bobres (bobres.co)	Diablo PRO (diabloiptv.ca)
PHTV Media (phtvmedia.co.uk)	Private IPTV Access (privateiptvaccess.com)
TVRovale (tvroyale.org)	Comstar Services (comstarservices.com)
PDS Live (pdslive.media)	Falcon TV (falcontv.tv)
247 Stream (247tvstream.com)	SSTV IPTV (sstviptv.com)
IPTV Smarters (iptvsmarterscode.com)	Tugo TV (us.tugotv.com)
3Click (3Click.tv)	Pelican Hosting (pelicanhosting.com)
IPTV Trends (iptvtrends.com)	Gemini Streamz (geministreamziptv.com)

Most of the piracy services are located outside the United States. It's worth noting that the payment for "BayouBengalTV" listed a Louisiana location. The company's website, https://bayoubengaltv.us, shows an address in Abita Springs, LA.

The twenty sites began charging a set monthly subscription fee ranging from $5.99 to $40 (which is Bayou Bengal) depending upon the site.

Within two weeks, other charges occurred. On February 22 – just eleven days after signing up for the first piracy streaming services, two charges of $17.21 each occurred listed as "GB Pay affectioni." Affectioni appears to be a woman's apparel store in Qingdao City, China. GP Pay is a mobile payment service.

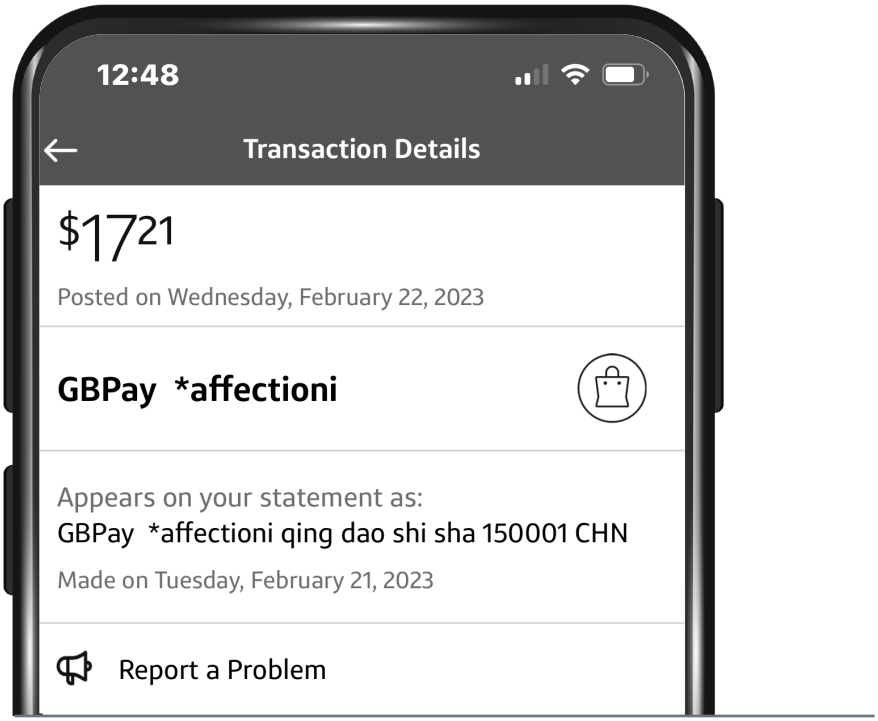

Image 1

Just a day later, a cash advance of $14.99 (along with an additional $3 fee) was made using the Wollito crypto platform. According to the credit card statement, the purchase originated in Vilnius, Lithuania. No other information is available.

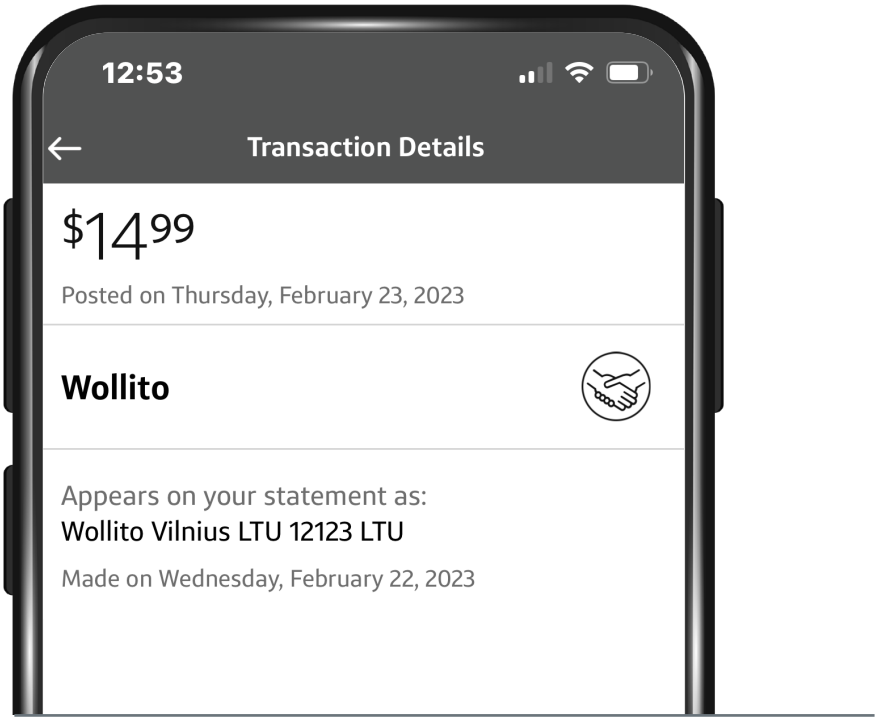

Image 2

The next illicit charge occurred on March 22, with a $16.60 purchase at a clothing store based in Hong Kong. The name on the charge was "clothingyoyo," which corresponds to the Clothing Yoyo outlet based in Sheung Wan, Hong Kong.

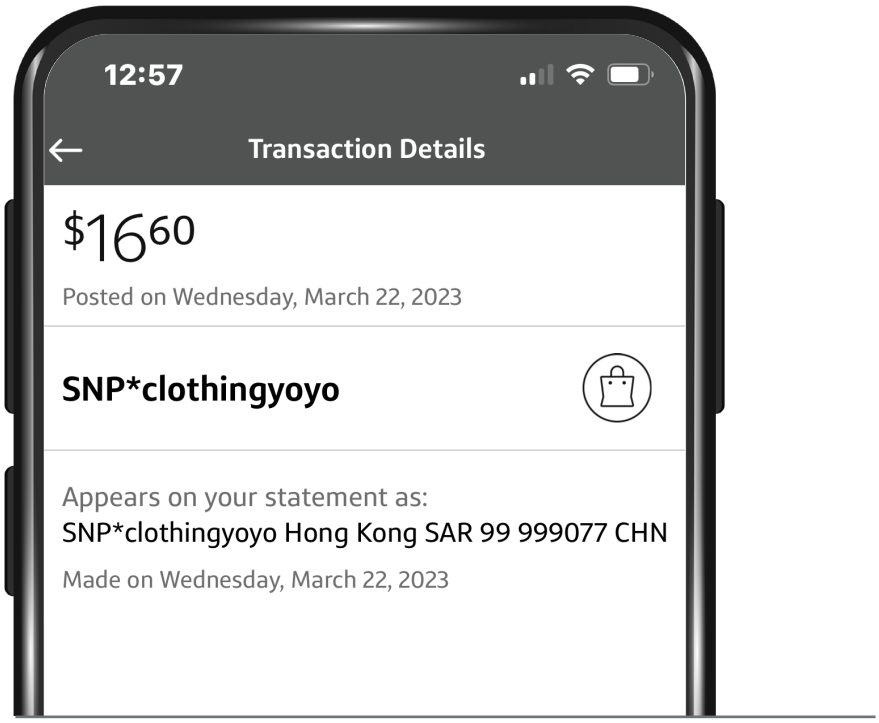

Image 3

The next unauthorized charge showed up on March 31 for "thedailygroceries." It originated in Jiaxing Shi in China. Although the name indicates its food-related, the website, thedailygroceries.com, which appears to correspond to the charge sells jewelry such as necklaces and bracelets along with handbags. Given that, it's not possible to know for certain what was illicitly purchased.

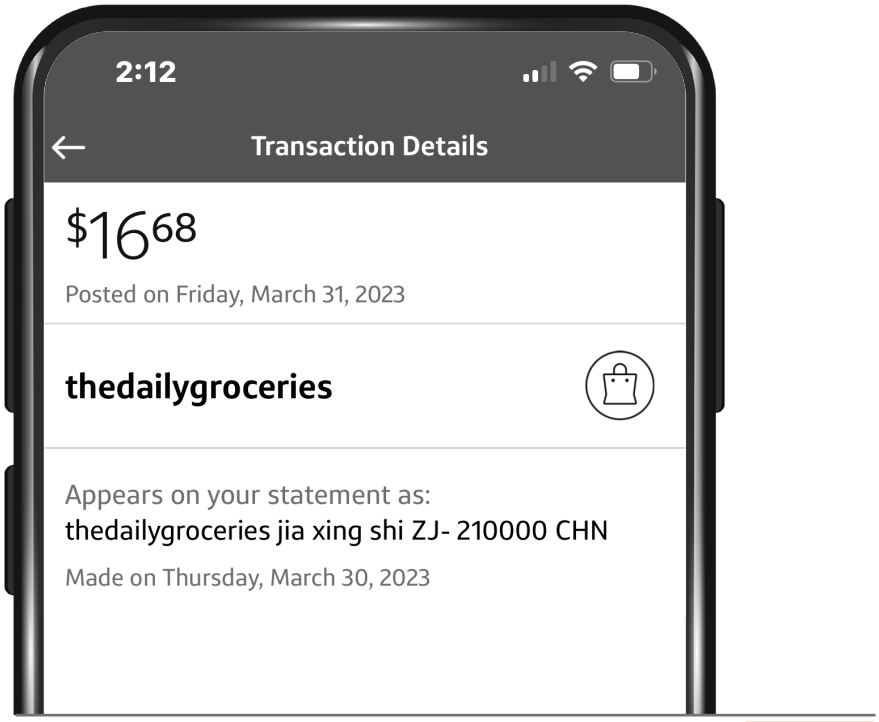

Image 4

Up until this point, the purchases had been smaller in nature. That changed on April 30 with attempts to make two larger purchases of $899 and $150. The nature of the purchases is not known because Capital One alerted the cardholder for approval, which was not given.

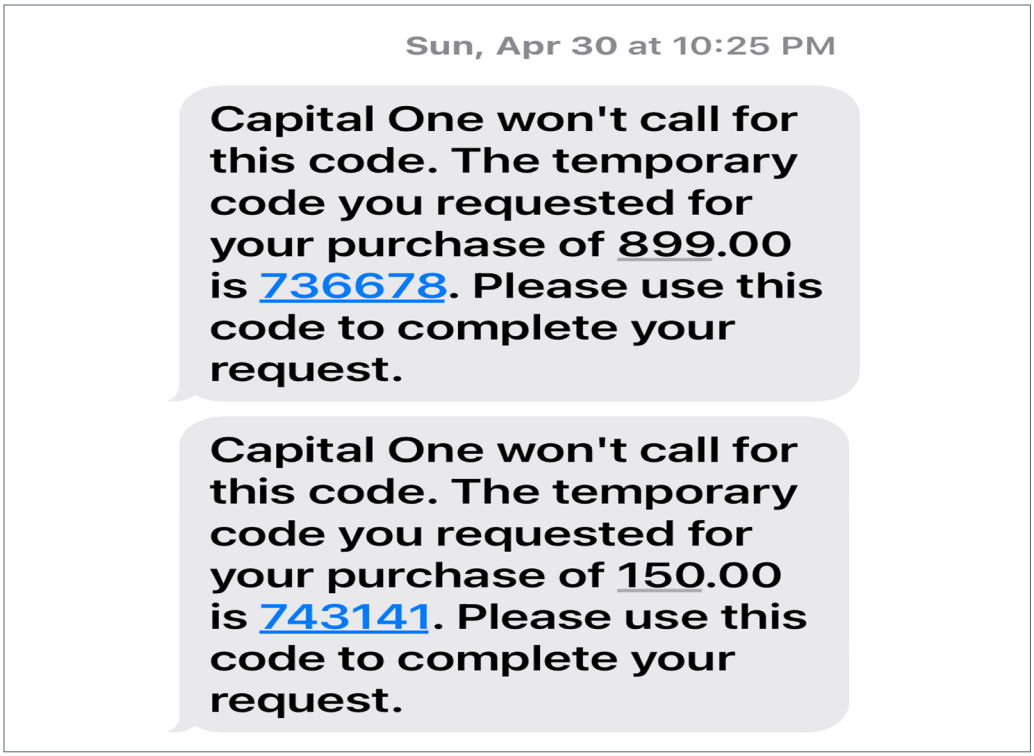

Image 5

Larger purchases continued in early May, with two at a Singapore-based apparel store. A purchase of $118.53 was processed on May 1.

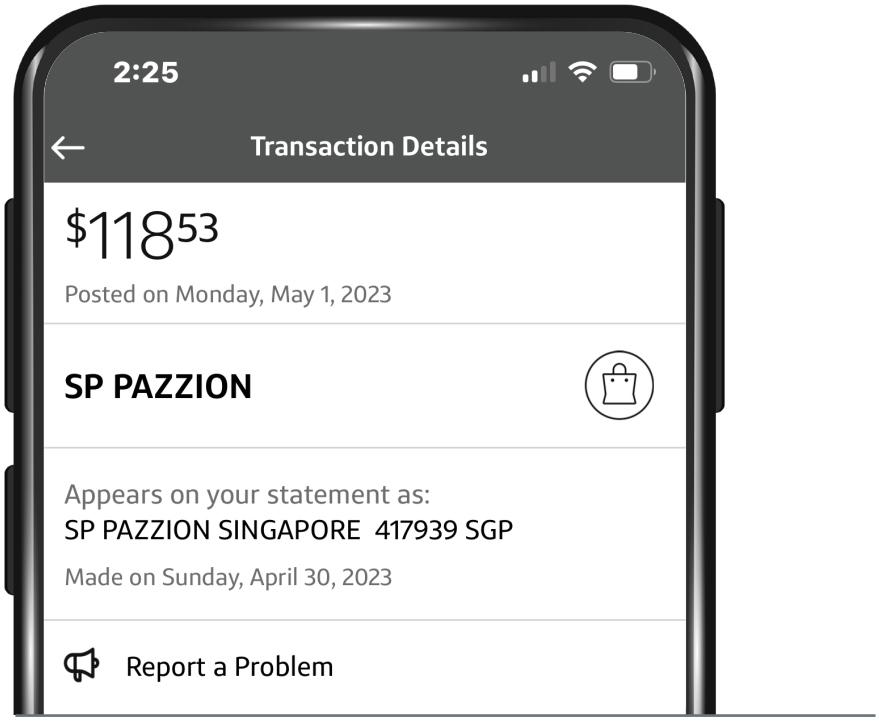

Image 6

A second purchase, on May 9, was processed for $244.78. According to its website, Pazzion sells apparel such as shoes, handbags, bracelets, and other accessories.

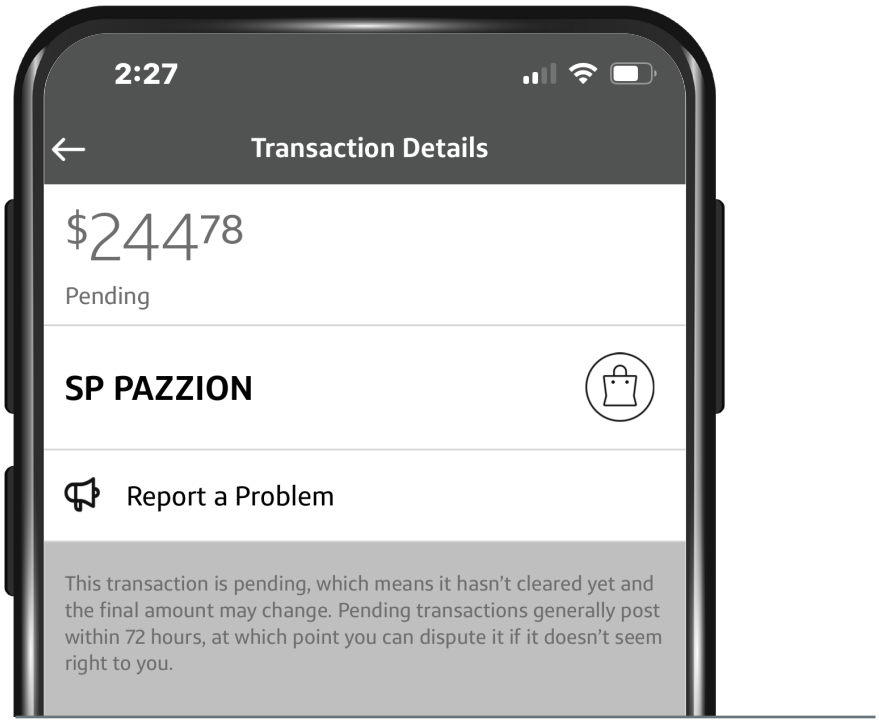

Image 7

In all, $1,495 in charges were attempted on the credit card over three months. It is important to underscore two things. One, the credit card was newly issued and used solely to sign up for piracy streaming subscriptions. Two, given there were twenty services, it is not possible to know the source of the fraudulent activity.

But given the unauthorized charges, it should make Internet users think twice before giving their credit card information to those operating illicit services.

Assessing the Risks

Credit card fraud is a scourge on consumers. Whether it's from an online purchase at a sketchy site or giving your credit card to a scheming hotel employee to a criminal stealing a card in the mail, it can create havoc on a person's finances. Americans filed 389,737 reports of credit card fraud with the Federal Trade Commission in 2021, the last year of record. And given how many don't report fraud, that is likely a fraction of the instances of Americans being victimized.

It's also big business. In May, the U.S. State Department offered a $10 million reward for information leading to the arrest of a Russian national accused of operating a platform where stolen credit card information is bought and sold.

To better understand the risks of piracy websites and apps, Digital Citizens commissioned a research survey that asked 2,330 Americans about how they get their entertainment. Roughly 1 in 3 Americans reported having watched pirated content at least once over the past year. Some relied on pirated content after canceling other legitimate streaming options or cable or satellite services.

About 1 in 10 who reported watching pirated content said they had purchased a subscription using a credit card to do so. That's where it gets interesting.

Seventy-two percent of Americans who said they used a credit card to purchase a piracy subscription service also reported having an issue with credit card fraud over the last year. That's an alarming incidence rate when you consider that only 18 percent of those who said they don't visit pirate sites reported a similar issue.

Experienced a Credit Card Breach	
	Yes
Used a Credit Card for a Piracy Subscription	72%
Don't Visit Piracy Websites or Apps	18%
Source: *Digital Citizens Survey Research of 2,330 Americans conducted 5/11*	

Credit card theft and identity theft are often related. And much like the correlation between visiting piracy sites and credit cards, there are indications that those who visit these illicit sites are also more likely to report an issue with identity theft. Americans who responded to the survey report those who visited piracy sites are three times more likely to report being a victim of identity theft.

Experienced Identity Theft	
	Yes
Visit Piracy Websites or Apps	44%
Don't Visit Piracy Websites or Apps	10%
Source: *Digital Citizens Survey Research of 2,330 Americans conducted 5/11*	

As previous investigations have shown, the risks go beyond credit card fraud.

The risk of malware is severe on piracy sites, in large part because illicit actors know that they can manipulate users either through fear (false claims about viruses) or enticement (getting something for free) to make a fateful click that compromises their devices. In fact, those who visit piracy websites and apps are five times more likely to report having an issue with malware over the last year.

Experienced an Issue with Malware	
	Yes
Visit Piracy Websites or Apps	46%
Don't Visit Piracy Websites or Apps	9%
Source: *Digital Citizens Survey Research of 2,330 Americans conducted 5/11*	

Piracy & Credit Cards: What to Do?

Nine million American households subscribe to piracy subscription services. They do so after being lured by the promise of inexpensive entertainment. In return, piracy operators offer them up to illicit actors to infect their computers so they can steal financial information, make them a ransomware victim, or exploit their identity. Now, we also know that credit card theft is a likely outcome of a person handing over their credit card information to a piracy operator.

The proliferation of piracy services into Americans' homes – and the damage they do – requires concerted action by federal and state governments, the credit card companies that piracy operators rely on, and consumers themselves.

It starts with payment processors that unwittingly help piracy operators accept payments from users reviewing their relationships with piracy services. While it's understandable that MasterCard wasn't aware it had merchant agreements with those operating the illegal businesses included in the reports, now it does. MasterCard should identify piracy operators, and, after determining if these businesses engaged in illegal acts, terminate the relationship.

The FTC must take piracy more seriously. When companies and organizations flagged how piracy websites were being used to spread malware, the FTC took steps to warn consumers. New research shows that interacting with piracy sites is dangerous on multiple fronts. The FTC should therefore prioritize warning Americans about online risks that can expose them to financial fraud.

Law enforcement should use the tools they have been given to launch criminal investigations. In 2020 Congress passed legislation to make piracy streaming a felony. Given that the piracy ecosystem is now a $2 billion industry, the Department of Justice should use that authority to target piracy operators. Doing so would be consistent with the DOJ's prioritization of cracking down on ransomware schemes. As mentioned above, ads on piracy websites and apps are a clever means criminals use to instigate ransomware attacks.

Lastly, consumer protection groups must create their own campaigns to warn Americans about the risks. The Digital Citizens Alliance is working with federal and state policymakers to create content and tools to raise awareness about the risk users take when they visit piracy websites and apps.

Research shows that when consumers are alerted to risks, many will modify their behavior. As a society, we shouldn't accept that being victimized by credit card fraud or malware is the price of operating online. Through a concerted public-private partnership, we can restore consumers' confidence in the digital world.

About Digital Citizens Alliance

The Digital Citizens Alliance is a nonprofit, 501(c)(6) organization that is a consumer-oriented coalition focused on educating the public and policymakers on the threats that consumers face on the Internet. Digital Citizens wants to create a dialogue on the importance for Internet stakeholders—individuals, government, and industry—to make the Web a safer place.

Based in Washington, DC, the Digital Citizens Alliance counts among its supporters: private citizens, the health, pharmaceutical and creative industries as well as online safety experts and other communities focused on Internet safety. Visit us at digitalcitizensalliance.org