Bahl&Gaynor
Investment Counsel

December 2, 2021

Your Identity Remains at Risk:

ID Theft on a Record Pace

By Glenn Warden
Chief Information Officer

U.S. online holiday shopping is expected to reach a record $215B this year; that's more than 12% year over year growth following an unprecedented surge last year.[1]

Be advised, as we place more items in our virtual carts, scammers are more than keeping pace. The Federal Trade Commission reported a 113% increase in ID theft cases last year over 2019 and anticipates the cost to Americans to grow by nearly $9B in 2021.

It was, of course, the pandemic that fueled the surge in 2020; the increase and extension of unemployment benefits made that sector an attractive target for scammers. But new credit card accounts are the next largest category of FTC complaints and remain a huge problem.[2] Fraudsters can steal your identity, apply for and receiving a new credit card in your name. Account takeover is another illegal, but increasingly popular move where criminal can steal money and/or access rewards from airlines, hotels, or merchants, even insurance policies.

Bahl & Gaynor offers our clients instructions to follow should they believe they are victims of identity theft. We're happy to share them with you, HERE.

Meanwhile, here are some important tips:

Things you can do to protect yourself from identity theft:

- Freeze your credit with all the major credit bureaus: Equifax, Experian and TransUnion. It's free, doesn't affect your credit score, and prohibits anyone pretending to be you from opening a new account.
- Guard your Social Security Number. Don't carry your card with you! Secure paperwork that includes your SSN.
- Ignore calls or emails asking for your personal information. You should initiate any communication that requires it.
- Don't open email attachments from unknown sources.
- Consider using a credit and identity theft monitoring service.
- Use strong passwords. Also, avoid obvious security questions (it's not hard to find your pet's name, city where you were born, or maiden name on social media.)
- Monitor your bank statements and credit card reports regularly.
- Hold your mail when leaving town.
- Shred statements containing personal information before trashing them, especially junk mail offering pre-approved credit offers. (Yes, people troll the garbage.)
- Add security software to your PC, laptop, tablet.
- Avoid connecting to public WiFi (i.e. airport, coffee shops) if possible.
- Consider a digital wallet. It's an app with digital, encrypted versions of your credit and debit cards. Bonus: it's contactless, so fewer health risks.
- Lock your mobile devices with a code or password. (Consumer Reports says only 36% of American smartphone users set a pin to lock their phones.)

[1] https://www.digitalcommerce360.com/article/online-holiday-sales/
[2] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime