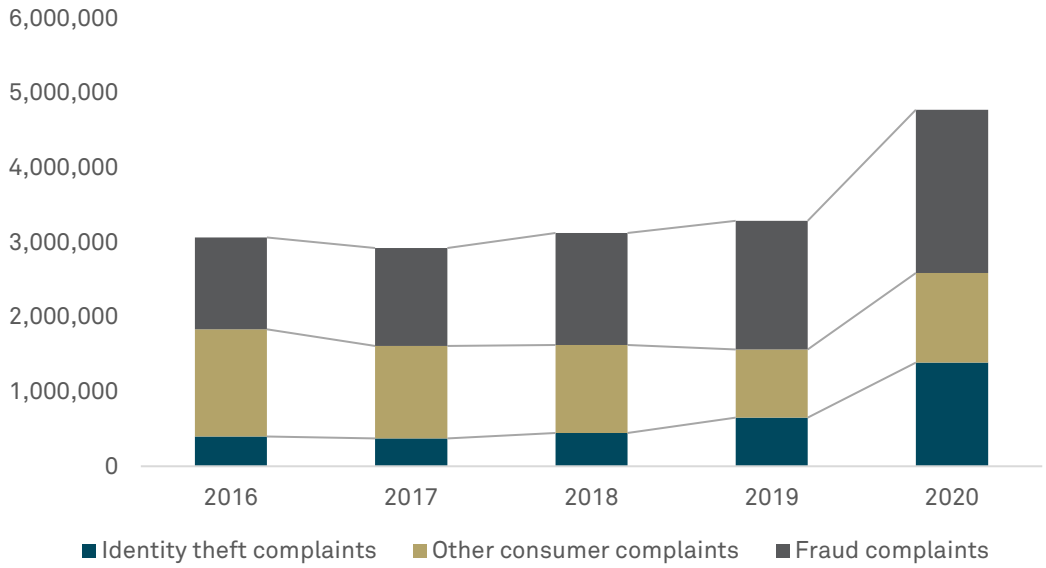
BNY MELLON
WEALTH MANAGEMENT

Banking on Solid Cybersecurity

Although the digital age has made many aspects of life easier, it has not come without its own issues. Rapid technological advancement, allowing everything from self-driving cars to contactless banking, has led to an alarming increase in the rate of identity theft.

Identity theft occurs when criminals are able to procure the personal information of victims through deception. As a result, wealthy individuals tend to be key targets. But scammers do not discriminate; almost half of Americans experienced financial identity theft in 2020, resulting in an astounding $712.4bn in losses.[1] Among various types of identity theft, credit card fraud and business/personal loans accounted for a combined 37.8% of cases.[2]

Fraud Complaints, 2016-2020



Source: Federal Trade Commission, Consumer Sentinel Network.
Percentages are based on the total number of Consumer Sentinel Network reports by calendar year. These figures do not include "Do Not Call" registry complaints.

While the numbers may seem alarming, there are ways to minimize cyberthreats. Banks are deploying a number of robust measures to combat the rise in cybercrime. But before we delve into what's being done, it's important to understand what you need protection against and how it can impact your wealth.

[1]Insurance Information Institute: Facts + Statistics: Identity theft and cybercrime. August 17, 2021.
[2]Ibid.

Types of threats

The most common ways cyberattackers gain access to sensitive financial information include ***ransomware***, ***phishing***, ***vishing*** and ***smishing***. The last three are a special kind of cybercrime, categorized as social engineering attacks. While you have likely come across these terms before, here's a brief refresher:

- **Ransomware**: Attackers deploy malicious software that threatens to publish or block access to a victim's personal data unless a ransom is paid.
- **Phishing**: Attackers attempt to impersonate a trusting entity, such as an organization or person, to obtain personal information by prompting victims to click an email link or open an attachment.
- **Vishing**: Attackers mask their phone numbers, pose as reputable entities and attempt to obtain confidential information from victims over the phone.
- **Smishing**: Attackers use text messages to collect information from victims by coercing them into clicking a link.

In each circumstance, cybercriminals attempt to trick victims into revealing account information that can lead to their assets. That's why it's important to bank with an entity which has the necessary cybersecurity infrastructure to protect your wealth.

What you can do

The first step of practicing cyber safety is to stay vigilant. Here are a few tips:

- Don't log in to your financial accounts on public computers, and don't access financial sites when using public Wi-Fi networks
- Don't use public charging stations or sync your phone with rental cars
- Don't answer unsolicited phone calls
- Don't blindly click on email links, social media posts and text messages
- Bookmark important websites and only access those sites via bookmark

Next, it's important to thoughtfully manage your passwords for online banking and services. You're likely aware of ***some*** protective measures, like refraining from password sharing and not leaving them where they can be discovered (such as a post-it note on your computer or a slip of paper in your wallet), but it might be wise to read our checklist of best practices, which provides everything you need to know about safe password management.

While many providers offer compelling banking services, consider speaking with your financial advisor to select one that offers an extra layer of protection against security breaches. A little preparation can go a long way. One of the things we do at BNY Mellon Wealth Management is offer free identity protection with our Total Wealth Checking Account. While we believe complimentary identity protection is an essential component of proactive cybersecurity for you and your family, our full suite of preventative measures is what truly differentiates the banking experience that we offer.

What we do

BNY Mellon Wealth Management deploys a rigorous authentication policy framework when clients initiate cash disbursements; demographic changes to information such as their home address or email address; changes to security-related and value-bearing instructions; and changes to call back phone numbers and upfront passwords. This includes step-up authentication on specific transactions with characteristics that look suspicious or high risk. We have a dedicated information security team of 541, which actively monitors accounts to block unauthorized access.

We also have a Know Your Customer (KYC) & Account Opening Group, which identifies and mitigates money laundering, as well as reputation and regulatory risks to the company. The team implements, controls and monitors requirements of the global Anti-Money Laundering (AML)/KYC policy through specific procedures as they relate to prospective and active clients.

Additionally, our employees regularly rehearse extensive business recovery and cyber incident response plans, as well as various hypothetical scenarios, to prepare for future threats. Our private banking clients receive the full benefits of our preventative measures, assuring rigorous protection every step of the way.

Using the most up-to-date encryption technology, BNY Mellon has kept pace with technological innovation to build on its 200-year track record of protecting the wealth of successful individuals and families across the world.