Information Security E-newsletter

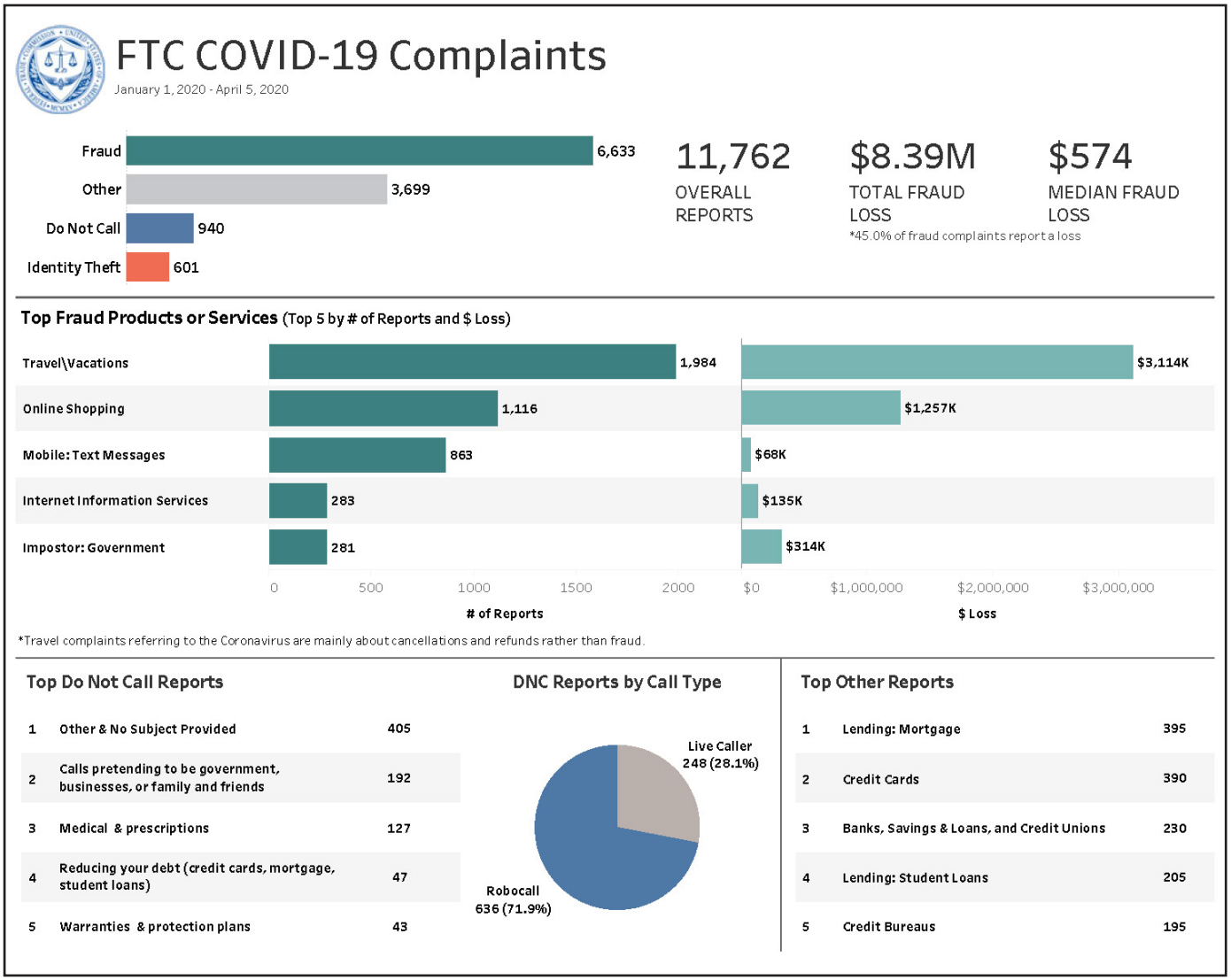
April 2020 | Issue 20.04

produced by
BankOnITUSA®

Stay Alert for COVID-19 Related Cyber Scams

Since January 1, 2020, the Federal Trade Commission (FTC) has had nearly 12,000 reported complaints related to scammers using the COVID-19 virus as a ruse to defraud people. The FTC's chart at the end of this newsletter illustrates that fraudsters are opportunistic and are using the COVID-19 virus event in their messaging.

- **Fraudulent Messages** – Fraudsters are sending messages claiming to be from the Centers for Disease Control and Prevention (CDC), World Health Organization (WHO), or other health entities. Some variations email a link to a fake look-alike website or direct you to download a document. Remember – do not respond to messages like these, and do not download anything or click on links in unsolicited email. It's the latest form of phishing aimed at stealing confidential data or installing malware on your network.
- **Business Email Compromise (BEC)** – We've warned previously about frauds perpetrated via business email. For example, an employee receives a message that appears to come from a company higher-up directing the person to wire money, transfer funds, or some other activity regarding movement of funds. In actuality, a con artist has spoofed a superior's email address or phone number. Why the renewed warning call on BEC scams? The coronavirus situation has resulted in a large number of legitimate, out-of-the-ordinary requests accompanied with the need to take action swiftly. As a result, a request that would have seemed out of place in early January might not seem so unusual in today's environment. That combined with the fact that many employees are working from home and cannot walk into the boss's office to ask about any unusual requests increases BEC risk. Stay alert, confirm requests and follow the procedures established by your financial institution.
- **IT Support Scams** – Support scams work similar to a Business Email Compromise (BEC) scam, but this time the call or message claims to come from a member of your technology staff asking for a password or directing the recipient to download software. These scams pose a particular problem now due to social engineering. The con artists are experts at manipulating human behavior to facilitate fraud and know you are likely distracted by changes in your routine. Taking advantage of the unfamiliarity of working from home and the overall COVID-19 situation, con artists do a quick online search and gather information to sell their story. For example, "I spoke with Fred, who said you were having a computer problem," or, "The meeting has been shifted to our new teleconferencing platform. Here's the link." Your best defense is to be aware of this type of fraud. And, if you are unsure if the caller is legitimate tell them you will call them back. Then call them back at a number you already have for them, not one they give you.
- **Know the Seller** – With many businesses scrambling for supplies, be wary of websites that mimic the look of well-known online retailers. They may claim to have the essentials you need, but in reality, they're fakes that take your order, and your credit card number, then disappear. The safer strategy is to type in URLs from legitimate sellers you know to be genuine. Be careful buying products online that are in high demand. Many scammers are pretending to sell items like hand sanitizers and cleaning supplies.
- **Phone Calls** – While working from home, employees are hearing a new crop of annoying – and illegal – robocalls. It's no surprise that fraudsters who already flout the law would try to exploit people's COVID-19 concerns to make a buck. Some of these fraudsters pitch bogus test kits and sanitation supplies. Others warn that "your Google listing is incorrectly displaying," leading you to believe your institution's phone number or address are incorrect online. Don't respond or press any number on your phone, instead, simply hang up.



Be aware that con artists and cyber attackers are continuously working, and you are an important part of the defenses your institution has in place.

Copyright © 2020 BankOnIT, L.L.C.
Disclaimer: This publication attempts to provide timely and accurate information concerning the subjects discussed. It is furnished with the understanding that it does not provide legal or other professional services. If legal or other expert assistance is required, the services of a qualified professional should be obtained.