7 summer fraud scams to avoid all year long

According to a recent Nilson report, global card fraud will reach $43.8 billion this year. While artificial intelligence, machine learning and other security innovations are helping to reduce fraud on all fronts, among the best weapons credit unions have in this fight is an informed, vigilant member.

Here are this summer's most prevalent financial scams that are catching consumers by surprise, which CO-OP Financial Services encourages you to share with your members.

1. Gift cards, secret shoppers and the allure of fake offers

This scam works as follows: consumers are drawn in by a phony e-mail or social media post to become a

"secret shopper" in exchange for some form of financial gain.

When a consumer agrees to participate, the fraudster seals the deal by delivering a very large counterfeit check. The criminal then asks the consumer to deposit the check and purchase gift cards with the funds – keeping a small portion of the proceeds as compensation for being the "secret shopper."

The victim here (a loose term, considering that most people will realize this is a scam!) is asked to e-mail photographs of the gift cards, front and back, so the criminal can use them immediately – before the counterfeit check has a chance to bounce.

Takeaway: The bounced check and all associated damages are the responsibility of the consumer because the criminal and his or her e-mail address are long gone by the time the check bounces.

2. "You can never be too rich or too thin" – and other e-mail scams

Some consumers are attracted to "get rich" and "get thin" offers, and unfortunately an age-old diet scam has surfaced again, targeting consumers with spam e-mails. When an unwitting consumer signs up for the "self-improvement" deal, that individual agrees to recurring billing for the proposed service.

Takeaway: This ongoing billing arrangement is difficult to stop. And, in some cases, the stolen payment card information is used for other fraudulent purposes.

3. Account takeover schemes

This scheme is dangerous for both credit unions and service providers and to their members. Social engineers, often armed with data from recent breaches, call into financial institutions on a regular basis, posing as customers or members looking to take over their accounts. And, it can be difficult for credit union employees to tell the difference because these criminals dial in with answers to the member's authentication questions (which they have sourced from the dark web).

Takeaway: It's important to come up with dynamic challenge questions that are atypical. Credit unions should also instruct employees to put any suspicious caller on hold and then place a separate call to the

member so his or her identity can be verified.

4. Counterfeit money orders

Fake money orders are frequently used for online purchases from websites like Craigslist. The problem is that high-quality counterfeit money orders are hard to distinguish from the real thing.

Takeaway: Credit unions should advise any member holding a potentially counterfeit money order to call the U.S. Postal Service verification line at 1-866-459-7822. The U.S. Postal Service can verify the authenticity of money orders 48 hours after they are issued – and they can also offer tips on how to recognize fake money orders in the future.

5. "MSN" help desk fraud

This form of fraud is usually directed at the elderly. A criminal calls an unsuspecting consumer and warns that his or her PC – however seldom used – is riddled with viruses.

The fake technician offers to assist, and then dispatches the victim to a local big box store to buy prepaid gift cards which are given as payment for the tech support services.

Takeaway: Losses to elderly victims of this scam can soar well into the thousands – and the criminals are willing to take every nickel without remorse.

Some big box stores have started to try and identify consumers who may be embroiled in these scams, but they can run into roadblocks when victims are either mentally incapacitated – or reluctant to admit they have fallen for a scam.

6. Card cracking

This rip-off scheme typically victimizes our youth. A fraudster reaches out to a young person via social media and convinces the potential victim that they can both benefit by helping each other out – with the young account holder receiving a small sum – $100 or so – as compensation for cooperating with the

fraudster.

The victim then gives the criminal access to his or her online banking credentials, so the criminal can deposit counterfeit checks into the account.

The fraudster also typically requires the usage of the account holder's debit card and, in some cases, accompanies the co-conspirator to an ATM to perform withdrawals against the counterfeit checks that have been deposited. This is especially troubling if the account holder is a minor in the company of an adult criminal.

Bottom Line: All financial damages, including non-sufficient-funds checks, fall back onto the young consumer. And that easy $100 profit? It was fake as well.

7. Direct mail scams

Bogus – but official-looking – letters are delivered every day to random consumers with stern requests for social security numbers and other personally identifiable information.

Some of these letters are printed on what looks like big bank letterhead and, in all cases, there is at least one "official looking" hard-copy form that the consumer is asked to fill out and return.

Takeaway: The addresses on these letters and the return envelopes provided are criminal addresses. They are not P.O. boxes belonging to actual businesses.

The main objective here is identity theft. This scam can be very convincing to consumers because the U.S. Postal Service has not been a criminal mainstay since the proliferation of e-mail in the mid-1990s.

Bottom Line: An informed consumer is an empowered one. Teaching members to recognize the signs of fraud will both reduce their risk and inspire their trust.

Contact us to learn about CO-OP's fraud and cybersecurity solutions.

Learn best practices for protecting your credit union and members against fraudsters at our next Fraudbuzz webinar on August 16: register now.

John Buzzard

John Buzzard is Fraud Specialist/Account Executive for CO-OP Financial Services, a financial technology provider to credit unions based in Rancho Cucamonga, Calif. (www.co-opfs.org). Buzzard can be reached ...
Web: **HTTPS://WWW.CO-OPFS.ORG**