SUBJECT: RESPONDING TO FRAUD ATTEMPTS ON MOP SITES

Over the last 7-10 days we have seen a batch of increased activity around MOP that demonstrates how MOP and identity thieves are starting to intersect more than ever. While most CUs with a MOP site have probably encountered a handful of sketchy apps by now, the impact over the past weekend resulted in about 250 fraudulent new memberships via one site, with smaller-scale events occurring at other MOP sites as well.

What Happened

In a nutshell, these bad actors apparently used stolen identities to create new memberships online. They used this stolen data to pass ID verification and then enrolled in online banking. By examining It's Me 247 Optics data, we were able to see them navigating to share rate boards, opening a checking account, and enrolling in bill pay.

They then used bill pay to attempt to pull funds from these new checking accounts and send them to another financial institution via ACH payments. Since the amounts ranged from $99.50 to $499.50, we surmise they were likely looking to access any courtesy pay limit that would have been made immediately available for new checking accounts. (Since this was not the case these items all hit the credit unions' ACH exceptions lists.)

Our Initial Response

Since the identities being used to open memberships were in fact real people, there was nothing that the software was doing incorrectly. People were being approved based on answering questions correctly; it just wasn't that person who was actually doing the applying.

Out of an abundance of caution, however, based on the noticeable uptick in volume over this past weekend we elected to temporarily suspend MOP opening processes. (*An alert was posted on Monday morning the 24th*.) Our thought was this would interrupt the fraudsters' efforts and encourage them to direct their attention elsewhere. We also hoped this would serve to get your attention, to encourage you to review your approach to verifying new members through this channel.

Also, in an attempt to set up another speed bump in the process, on Feb 20th we made a minor change to the MOP flow: we now force the completion of the funding step (assuming that's been activated by your CU) before enabling the temporary password that makes it possible to finish the online banking login process. None of the submissions we monitored have taken the trouble to fund the memberships...at least not so far.

What You Can Do Now

Automated underwriting for online membership requests is always a balance of using both technology and back-office verifications. Here are some ideas to consider:

- Since scammers are upping their game and using real stolen identities to test your systems, perhaps **tightening your Experian Precise ID settings** would be a good idea. Review your configuration with Experian and potentially beef up the speed bumps and evaluation questions you are using.

- **Examine the procedures and additional verifications your employees perform** immediately after someone joins the credit union. Scammers are now expanding their reach to online and mobile tools, testing things like your bill pay, P2P, and A2A programs. They seem to be hoping that you set up courtesy pay limits on new accounts right away. Don't.

- **Watch the email alerts you get** about new membership openings. Have a rule of thumb for average volumes expected, and react quickly to changes in your trends.

- Scammers adapt quickly. These days new tools like bots allow them to automate application processes and push more volume at CU websites. You need to adapt as well, so you should **plan on regular, frequent reviews of your approaches**.

How to Get Your MOP Site Reactivated

If your credit union has reviewed your procedures and risk assessment for opening memberships online and feel comfortable reactivating the MOP verification, funding, and online banking enrollment segments for your MOP sites, contact Kristian Daniel at kristian.daniel@cuanswers.com for assistance. We've reactivated sites for several CUs already.

What We're Doing Next

Here are some new things we'll be doing over the coming days and months:

- Looking into creating a new set of **reasonableness tests**, designed to block new memberships based on data that signals you don't want an applicant to be automatically approved (such as state, ZIP code, etc.), or based on an out-of-the-ordinary rise in activity on the site (compared to memberships processed in the last hour, day, month, etc.), to slow the roll of the automated process.

- Reviewing **live-person testing tactics** from Google.

- Reviewing **tech that could validate uploaded ID documents**, as well as live-person testing solutions from vendors like Mitek and ID-Pal.

- Reviewing making the **MOP on/off switch** available to CUs, so if you detect a spike in seemingly fraudulent activity you can flip the switch yourself without having to call us.

- Considering a configuration that could **temporarily block certain online/mobile features** for a period of time after a new membership is opened, while you get to know and develop a track record with your new member.

In the long run we foresee that MAP/MOP will add several new elective services to this process, **optional add-ons** you can activate or not according to your risk tolerance and budget. The goal is to let CUs append our software with additional technical solutions as well as things like validation services from AuditLink, so you can continue to evolve your online approaches with an eye towards both convenience and security.

What else? If you have other ideas, let us know!

•END•

CONTACT **Client Services** • csr_team@cuanswers.com • 800-327-3478 • 616-285-5711

CONFIDENTIALITY NOTICE The information contained in this message or any attached document is confidential and intended only for individuals to whom it is addressed. If you received this message in error, please inform the above contact name immediately and destroy the message and any attachments. Any unauthorized use, distribution, or copying of this information is prohibited.