WHITEPAPER

Mobile Banking Fraud Trends:

FRAUDULENT CHECKS MEET REMOTE DEPOSIT CAPTURE

Guardian Analytics®

GuardianAnalytics.com

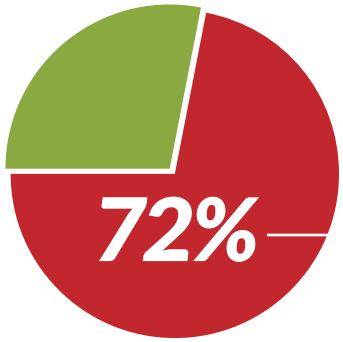
Mobile Banking Fraud Trends: FRAUDULENT CHECKS MEET REMOTE DEPOSIT CAPTURE

Fraudulent Checks Meet Remote Deposit Capture

Mobile banking use is on the rise, and as banking services grow, so do fraud attempts using mobile banking capabilities.

Fraudsters have repeatedly created schemes by blending old tactics with new technologies or new banking services. A recent technique involves a very old form of payment – checks – with a newer, but rapidly growing mobile banking service – remote deposit capture (RDC) – to commit check fraud.

Analysis conducted by Guardian Analytics across 400 financial institutions found that 72 percent of mobile banking fraud included use of remote deposit capture (RDC) and fraudulent checks.



Mobile banking fraud via RDC is impacting financial institutions of all sizes, and losses are escalating quickly:

- Attempted check fraud using RDC was reported by
  - –50% of community and mid-size banks
  - –90% of regional banks
  - –100% percent of superregional banks. [2]
- Banks suffering losses from consumer RDC activity increased 400% from 2012 to 2014. [2]

This dominant preference for RDC is of concern to financial institutions given the high availability and increasing utilization of this service.

- Mobile banking users expected increase from 1B to 2B by 2020 [1]
- 93 percent of FIs offer RDC to retail account holders (as of 2014) [2]
- The use of RDC will increase 98 percent from 2015 to 2016 [3]

The mobile banking scams leveraging RDC most frequently in use are the Sweetheart Scam and Fake Online Payday Lenders. This report details how these scams work, and how fraudsters are using mobile banking to commit check fraud.

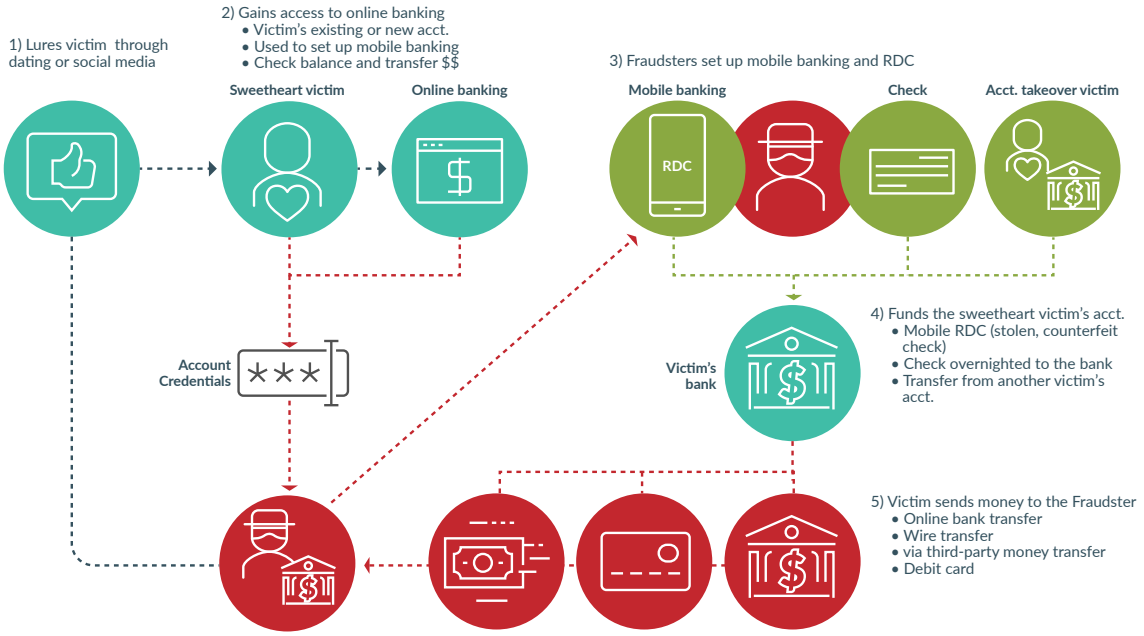
The Sweetheart Scam

Victims are romanced on online dating sites or social media networks. Once the scammer has hooked a lonely-heart, they ask the victim to help with completing a financial transaction exploiting online banking and newer technologies such as mobile banking and remote deposit capture (RDC).

The sweetheart scam begins when the fraudster forms a relationship with the victim via an online dating site or social network. Once winning the confidence of the victim, the fake paramour asks for online banking access, using a sob story or simply asking for help (e.g. needing to pay a business for goods received). In some cases, instead of providing access to an existing account, the victim opens a new account.

The fraudster sets up mobile banking for the account, including the ability to use mobile RDC, and then uses RDC to make a deposit into the victim's account, often using stolen, counterfeit, or cashier's checks.

The fraudster then uses online banking to check the account to see when the deposit has cleared, often checking frequently so that he can quickly complete the scam.



Once the check has cleared, there are three ways the fraudster gets the money out (see diagram, part 5).

A) The fraudster uses online banking to initiate a wire or to transfer funds into one of his existing accounts at another financial institution.

B) The fraudster asks the victim to send him the deposited money by cashing out and then using a third-party money transfer service.

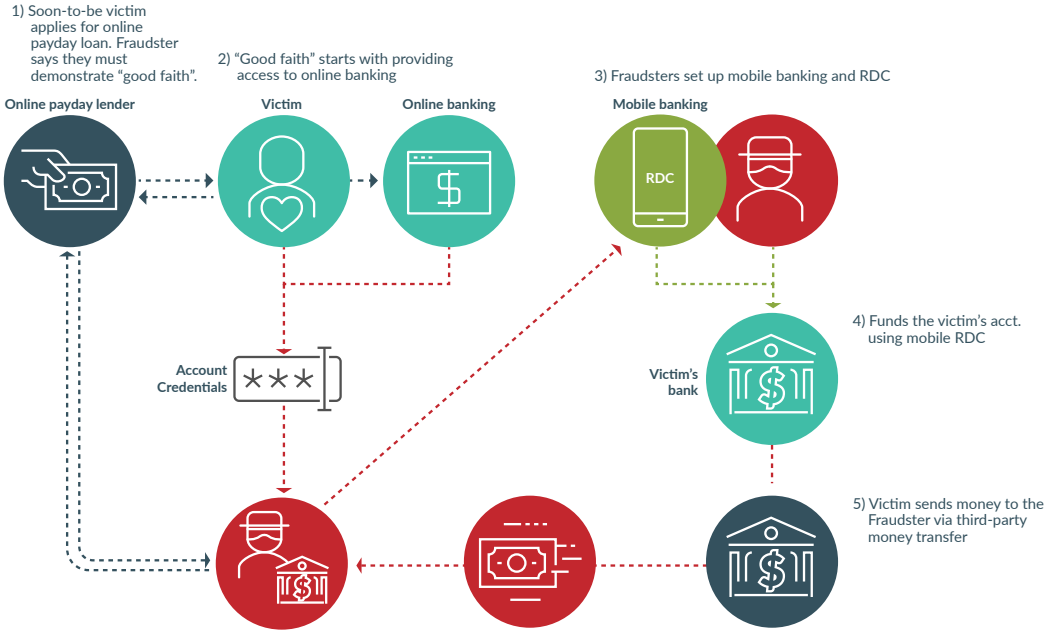
C) The fraudster asks the victim to send him a debit card, enabling the scammer to cash out at an ATM.

Fake Online Payday Lenders

This scam starts with a person signing up to receive a payday loan from an online vendor. A fraudster, posing as an online payday lender, tells the applicant that in order to receive a loan he must demonstrate "good faith." This "demonstration" starts with enrolling in online banking and then providing the fake payday vendor the online banking credentials.

The fraudster then uses the online banking credential to enroll the victim in mobile banking and subsequently uses RDC to deposit checks into the account. The hopeful soon-to-be- recipient of the loan is instructed to go to the bank, withdraw the funds and send the money back to the payday loan company through a third-party money transfer service.

By demonstrating this "ability to pay" the victim will then supposedly receive his or her payday loan. It comes as no surprise that the deposited checks are fraudulent, the money is gone, and the victimized account holder is unable to repay considering the victim was seeking a payday loan in the first place.



Prevention Tips

Here are some guidelines for using behavioral analytics to prevent the sweetheart scam, fake online payday lender scam, and other attacks using mobile RDC.

- **Monitor the IP address.** Look for unusual activity, such as logging into mobile banking from many different locations. In one case, an FI noted 28 logins in a 24-hour period from 4 different IP addresses.
- **Monitor the source of RDC activity.** In these schemes, the fraudster uses RDC to make the deposits, so the location from which the deposits are made and the IP address will likely be inconsistent with what is typical for the victim.
- **Review the endorsement.** In these attacks, the endorsement on the back of the check is usually abnormally correct – there is a full name endorsement (usually including middle names), the endorsement is a printed name, there's a full account number, and it includes "for mobile deposit only."
- **Scrutinize users of any new service.** First time use of a new service such as RDC or mobile banking warrants closer scrutiny, especially if the client signs up for both in rapid succession. This especially is true for users whose profile doesn't conform to the typical user of the service, such as an elderly customer suddenly needing mobile capability or younger users with infrequent deposits suddenly requiring RDC.
- **Flag any unusual deposit patterns.** Established banking customers usually will have a routine pattern for the timing and amounts of their deposits. Monitor mobile deposits for unusual frequency, time of day, amounts, device, or speed of registration-to-deposit timing.
- **Review new account openings.** Look for new accounts opened by existing account holders, with no obvious reason for needing the new account, followed by substantial deposits.
- **Go beyond a simple confirmation of the transaction.** When speaking to account holders about these suspicious activities, ask questions that will help uncover if the client is being victimized without their knowledge. For example, ask where the funds are going, for whom, and for what purpose.

[1] Juniper Worldwide Digital Banking report
[2] ABA 2015 Deposit Account Fraud Survey Report
[3] Celent State of Remote Deposit Capture 2015 report

ABOUT GUARDIAN ANALYTICS

Guardian Analytics is the pioneer and leading provider of behavioral analytics and machine learning solutions for preventing banking and enterprise portal fraud. Hundreds of financial institutions have standardized on Guardian Analytics' innovative solutions to mitigate fraud risk and rely on the company to stop the sophisticated fraudster attacks targeting retail and commercial banking clients. With Guardian Analytics, financial institutions build trust, increase competitiveness, improve their customer experience and scale operations. Guardian Analytics is privately held and based in Mountain View, CA. For more information, please visit www.guardianananalytics.com. Guardian Analytics is a registered trademark of Guardian Analytics, Inc.

650.383.9200 2465 Latham Street, Mountain View, CA 94040

Guardian Analytics®

GuardianAnalytics.com