Educating Your Customers About SIM Swap Fraud

mobile banking risk management phishing

Summary: SIM swapping has increased sharply over the past years. In order to keep their customers safe, community financial institutions need to take proactive and preventative measures, including communicating with customers through two independent means on transactions, warning of red flags, and advising on safe social media usage.

The only insect that can turn its head is the praying mantis. Its average life span is 1Y and there are 1,800 species around the world. Gardeners often welcome these insects since they eat many garden pests. Criminals that prey on bank customers through their phones are another kind of pest we focus on today.

Criminals who take over your customer's phone can tap into their bank accounts and make off with their funds. Unfortunately, instances of **SIM swapping** have risen sharply over the last few years.

Defining the problem

SIM swapping occurs when a thief impersonates a user and attempts to convince cell phone companies to move the user's data to a SIM card in the thief's possession. Once an attacker gains control of the user's phone number, it lessens hurdles associated with gaining access to the customer's accounts. The two-factor authentication checkpoint that many financial institutions (FIs) use to protect accounts is now in the hands of the thieves. The thief can now easily recover the passwords needed to access the user's bank accounts. In short, it's a way to hijack accounts and steal money. Thieves can swiftly empty bank accounts, run up credit card debt, and destroy your customer's credit.

Widespread vulnerabilities exist

Getting away with this theft is easier than you might think. A Princeton University academic study from last year found major US prepaid wireless carriers are especially vulnerable to this type of attack. Despite the safeguards that carriers have enacted, the barriers to thievery aren't full-proof.

Take proactive and preventative steps

FIs rely on carriers to defend against SIM swap. Still, there are steps that can be taken by FIs to mitigate the problem. Here are a few suggestions.

- **Communicate with customers** about every financial transaction through two independent means, such as text and email.
- Proactively warn customers about these red flags:
  - **Phone call or text blockages.** Customers who out-of-the-blue can't make or receive calls or text messages, should consider themselves potential SIM-jacking victims and immediately contact their wireless provider.
  - **Odd activity notifications.** Look out for email alerts or phone calls to backup numbers from mobile phone providers regarding suspicious activity.

- **Advise on safe social media usage:**
  - Encourage customers not to publish their phone numbers on social media profiles.
  - Advise customers to limit the amount of personal information on these platforms.

- Continue to remind customers that your institution will never call or email to ask for their personal sensitive information. **Instruct them to ignore phishing emails** and report them.
- **Encourage customers to promptly report potential SIM swapping** issues to their phone carrier. They should also visit https://www.identitytheft.gov/ for other steps to follow.

While this may seem a long-shot for your customers, it is a growing fraud issue. Make sure to keep communicating about fraud risks with your customers to keep them sharp at all times.

IMPROVED EFFICIENCY WITH CHECK IMAGING FOR CANADIAN CASH LETTERS

PCBB's enhanced cash letter service for Canadian checks can help your institution minimize its credit exposure, increase operational efficiency, and deliver faster fraud notification. Learn more about our check imaging for Canadian cash letters.