



Four Strategies To Fight IVR Fraud

🔗 technology fraud protection employees

Summary: Does your institution use an interactive voice response system? Most do. While very effective at providing round-the-clock customer service, fraudsters are now using them to infiltrate customer accounts. Scammers love IVRs, so we explore four strategies to help you fight this type of fraud.

Do you remember the olden days when cameras were stand-alone devices that you had to lug around just in case you needed it? Well, since today is National Camera Day, we thought it was appropriate to remind you how far we have come with cameras. These days, it is easy to capture a picture — just pull out your smartphone!

Smartphones make everything easy, even actual phone calls. When a customer calls a financial institution (FI), they typically go through a phone tree and an interactive voice response (IVR) system. FIs have spent time and effort making IVRs more user-friendly for customers. But making IVRs more customer-friendly and feature-rich can also make them more vulnerable to fraud. An [estimated 60% of online fraud starts with or includes a call to the IVR](#). In another survey, 37% of bank executives said they had seen [evidence of fraud](#) coming through their IVR system.

Why scammers love IVRs

The characteristic of IVRs that FIs find so appealing is the ability to handle large volumes of calls, any time of day or night. But that is exactly what makes IVRs so susceptible to abuse. Scammers can make hundreds of calls to an institution's IVR, looking for a way to navigate into an account. They employ bots and robocalling to probe IVRs, testing thousands of PIN numbers until they find one that works. In other words, they try repeatedly to find a hook that allows them to impersonate a real customer. Oftentimes, they move from the automated responses to a live agent and try to trick the agent into revealing sensitive information — such as a security word like a dog's name. All it takes is one slip and a scammer has the key to unlock an account they can loot. A break-in can also lead to more serious damage, if the cybercrook can get into other parts of an institution's system.

Strategies for community financial institutions (CFIs) to protect themselves

1. **Improve monitoring of the IVR.** You may be monitoring your IVR system, but with the growing fraudulent activity, you will need to step it up. Constant monitoring of IVR for signs of fraudulent activity like repeated calls from the same number or calls from a number that can't be authenticated as real, can help a CFI spot a fraudster before he gets very far.
2. **Use security solutions that are designed to spot fraud in IVR.** These solutions should provide an umbrella of protection by identifying accounts being targeted by possible scammers and callers who may be mining for data, instead of seeking customer service. These should also analyze data in real-time and issue alerts about suspicious activity.
3. **Ensure agents who receive calls through IVR are trained** in spotting suspicious calls and can respond. Fraudsters often enter through IVR and use bits and pieces of information to try to impersonate real account

holders. Then they try to trick the agent into revealing more information about the account. Agents need to be educated so they don't mistakenly fall for this.

4. **Make sure your institution's IT security team is trained** to act quickly in dealing with these security alerts. Specific protocols should be in place and tested, as with all others.

IVRs can be valuable tools in a CFI's ability to provide 24-7 customer service. But their durability in responding to customer calls can also present a security risk. Balancing customer ease of use with tight security is the key to an effective IVR.

READY FOR SOFR?

Financial institutions need to be prepared for the transition from LIBOR to SOFR. We make it easy by supporting LIBOR, SOFR, and fed funds. Learn more in our [SOFR Resource Center](#).

ECONOMY & RATES

Rates As Of: 06/29/2021 05:47AM (GMT-0700)

Treasury	Yields	MTD Chg	YTD Chg
3M	0.05	0.04	-0.04
6M	0.06	0.03	-0.03
1Y	0.08	0.03	-0.03
2Y	0.26	0.12	0.14
5Y	0.92	0.12	0.55
10Y	1.51	-0.09	0.59
30Y	2.13	-0.16	0.48
FF Market	FF Disc	IORR	
0.10	0.25	0.15	
SOFR	Prime	ORER	
0.05	3.25	0.08	

Copyright 2021 PCBB. Information contained herein is based on sources we believe to be reliable, but its accuracy is not guaranteed. Customers should rely on their own outside counsel or accounting firm to address specific circumstances. This document cannot be reproduced or redistributed outside of your institution without the written consent of PCBB.