Accident Ahead – Insufficient Security Leads to IVR Fraud

cyber security

Summary: Many financial institutions rely on interactive voice response to provide customers secure access to information about their accounts. While extremely efficient for customer service, insufficient security measures can also make them a gateway for fraud. We highlight several areas that bankers should be aware of regarding IVR fraud.

The global positioning satellite app, Waze, has become extremely popular in recent years. Not just because of its ability to map out a route to a destination you ask it to navigate to, but. its additional features to locate restaurants, gas stations, hotels and other attractions that are in close proximity to the route you are traveling. Perhaps its most useful feature is the fact that it notifies drivers that there is an upcoming traffic jam or accident, while on route and can map out an alternate route.

The ability to get around roadblocks is extremely valuable for drivers, particularly those in a hurry to reach their destination. Similarly, in banking, there are times when customers want the ability to circumvent obstacles, such as the interactive voice response (IVR) systems used by many financial institutions to provide customers secure access to information about their accounts. While IVR systems provide financial institutions an inexpensive, user-friendly way to access account information and execute simple tasks, insufficient security measures can also make them a gateway for fraud.

IVR weaknesses. Unfortunately, cybercriminals have worked out ways to use IVRs for their own benefits as well., Indeed, 76% of organizations that rely on IVR systems have had experiences with scammers using them to access customer information or as a means of fooling live customer service agents into unintentionally revealing account specific information. And that number is only growing: as many as one in every 40 calls to an IVR system is a high-risk interaction with a scammer.

Protective Measures. The most important thing organizations using IVR can do to protect against fraud is to educate customer service representatives about the ways that criminals can use these systems to their advantage. Following are a few things organizations should be aware of regarding IVR fraud:

1. **Challenge:** One tactic used by criminals is known as **account enumeration reconnaissance**, where sophisticated algorithms can rapidly pull usernames from computer dictionaries to pinpoint the identity of an email domain – up to 700 per second. Using this method, fraudsters are often able to access enough details to circumvent the knowledge-based authentication questions that financial institutions typically rely on.

Possible solution: The security that organizations employ to protect against IVR fraud should incorporate artificial intelligence that can identify red flags such as multiple calls from the same number, blocked numbers or numbers that appear to be masked.

2. **Challenge:** Customer service representatives should understand that just because an IVR system has routed a caller through to them doesn't mean that caller is who they claim to be.

Possible solution: Further verification is critical, particularly since scammers can glean basic password information or answers to security questions from social media posts. Similarly, representatives need to be reminded of the importance to never volunteer any information about a customer's account during such interactions and to always remain on the defensive.

3. **Challenge:** Another popular tactic among criminals is to contact consumers posing as a bank representative looking to verify a suspicious charge, while a second person is calling a real customer service representative at your institution at the same time. In such instances, once the call is transferred over to a legitimate customer service representative at your institution, the criminals will remain on the line and record all the KBA answers needed to access the customer's account.

Possible solution: To protect against this scam, financial institutions should remind customers about the ways that your organization will and will not contact them regarding suspicious activity and encourage customers to call your organization directly if anyone ever contacts them by phone.

IVR fraud isn't limited to systems that allow customers to implement financial transactions, as criminals can still glean information from those that don't. Implementing software that monitors IVR systems is critical. While IVR has certainly helped provide a more seamless customer experience, it's important to always protect your customers – and your institution – from IVR fraud.

SHARE THE BID WITH A COLLEAGUE

Would someone at your financial institution want to receive our complimentary BID publication? Share the BID.

ECONOMY & RATES

Rates As Of: 06/10/2022 05:43AM (GMT-0800)

Treasury	Yields	MTD Chg	YTD Chg
3M	1.30	0.14	1.24
6M	1.81	0.17	1.62
1Y	2.41	0.33	2.02
2Y	2.96	0.40	2.22
5Y	3.18	0.36	1.91
10Y	3.10	0.25	1.59
30Y	3.17	0.13	1.27
FF Market	**FF Disc**		**IORB**
0.83	1.00		0.90
SOFR	**Prime**		**OBFR**
0.75	4.00		0.82

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.