BIOCATCH
Less Friction. Less Fraud.

Combating Cross-Channel Fraud with Behavioral Biometrics

Data Sheet

Cross-Channel Fraud in the Banking and Financial Services Sector

As the fraud landscape continues to expand rapidly, together with a surge in application fraud, credit card/payment fraud and social engineering manipulations, the banking and financial services sector is facing a new kind of threat: cross-channel fraud.

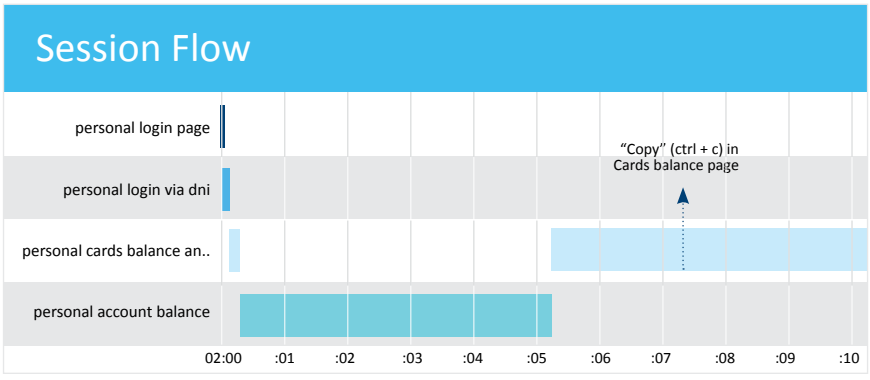
Cross-channel fraud is an advanced attack method in which the fraudster steals a user's credentials and personal information from one channel, in order to commit fraud in an associated channel and/or account. The extensive use of multi-channel banking and financial services has exacerbated the problem, as cyber-criminals use advanced attack techniques to exploit vulnerabilities of one channel and to steal funds and personal information from other related-channels.

Recent forms of cross-channel fraud have involved money transfers to fake deposits or mule accounts, followed by a cash withdrawal from an automated Teller Machine (ATM). Many times, entirely innocent third parties have been exploited to withdraw funds.

The main problem that the banking and financial services industry is facing pertains to the weakest link in any organization's security posture: the human factor. Customers are accustomed to assume that financial institutions and services have robust safeguards and security policies. Thus, customers sometimes do not question the legitimacy of fraudulent and deceitful messages/calls which are part of social engineering schemes - and provide credentials and sensitive information. After the fraudster harvests the victim's credentials, he often uses the stolen data to carry out the fraud in a different online channel.

Successful Deployments: Leading Banks in Spain and the UK

Leading financial institutions in Europe have deployed our solution with the aim of detecting fraud that begins in one online channel and that is later carried out in another. For instance, one of our customers in Spain is using the system to detect whether a fraudster illegally accesses the user's online banking account, then goes to the credit cards balance section to copy the user's credit card number and expiration date – this can be later used for eCommerce fraud. The combination of abnormal behavioral patterns with a risky context is a highly accurate method of detecting cross-channel fraud.



SAMSUNG SAMSUNG SDS AMERICA

A leading financial institution in the UK is also using our solution to detect cross-channel fraud. In this case, the customer also receives periodic reports, which include alerts on high-risk non-monetary activities. These reports are instrumental in preventing fraudulent activities before they happen, but are also effective in preventing fraud in related online channels.

Cross-Channel Fraud Prevention with Behavioral Biometrics

With cyber attackers becoming much more sophisticated, security measures must get smarter too. The key is to implement security measures in multiple channels that can test the authenticity of users in ways that are difficult to replicate.

Mapping and monitoring these behavioral patterns in different sessions (new applications as well as existing accounts), the BioCatch platform generates a risk score based on real-time analysis in the digital channel, where fraud activity is growing rapidly. This risk score can be fed into an existing platform in a different customer channel, such as the call center, to provide another security layer against fraudulent activity and streamline operations.

Having intelligence on potential risky activity online can minimize the risks associated with social engineering and identity theft in other channels. For example, our solution can integrate with biometric technologies like voice recognition systems to provide a complimentary safeguard. The risk score coming from the voice verification system would be combined with our risk score (based on behavioral biometrics) to create a more robust and comprehensive fraud prevention solution. Moreover, this combination can detect fraud that starts in one channel (online) and then moves on to another (voice channel), or vice versa.

How Does Behavioral Biometrics Work?

The BioCatch platform authenticates users by who they are, rather than by what they know (e.g, passwords, security questions). Employing cutting-edge behavioral biometric technology, BioCatch analyzes more than 500 different behavioral patterns during a session (post-login) to determine whether the user is in fact the genuine user and not a human/non-human imposter. These parameters include:

- Cognitive factors such as eye-hand coordination, applicative behavior patterns, usage preferences, device interaction patterns and responses to Invisible ChallengesTM.
- Physiological factors such as left/right handedness, press-size, hand tremors, arm size and muscle usage.
- Contextual factors such as, transaction, navigation, device and network patterns.

After comparing the session data to the genuine user's profile, BioCatch provides a risk score in real-time that can be used as a standalone indicator, or combined with other threat detection systems. For cross-channel fraud prevention, the risk score can also be fed into multiple related-channels and accounts. Our solution reduces friction associated with authentication, increases end-user satisfaction, retention, and drives high conversion rates. Moreover, through better risk analysis, fewer transactions are declined, ultimately generating new revenue streams.

About BioCatch™

BioCatch is a cybersecurity company that delivers behavioral biometrics, analyzing human-device interactions to protect users and data. Banks and other enterprises use BioCatch to significantly reduce online fraud and protect against a variety of cyber threats, without compromising the user experience. With an unparalleled patent portfolio and deployments at major banks around the world that cover tens of millions of users to date, BioCatch has established itself as the industry leader. The company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks and e-Commerce websites across North America, Latin America, and Europe. For more information, please visit www.biocatch.com.

About Samsung SDS America, Inc.

Samsung SDS America (SDSA) is the U.S. subsidiary of Samsung SDS, a global IT solutions company. SDSA provides purpose-built technology solutions in the areas of enterprise mobility, security, advanced analytics, mobile sales productivity, and training. We enable our customers in the public sector, finance, retail, and other industries to achieve greater freedom, more operational efficiency, and smarter decision making as the driving force for their competitive advantage. SDSA is headquartered in Ridgefield Park, NJ, with offices in Herndon, VA, and San Jose, CA. To learn more about Samsung SDS Biometric Solutions visit www.samsungsdsa.com or email us at bd.sdsa@samsung.com.

Contact Us

www.biocatch.com info@biocatch.com @biocatch www.linkedin.com/company/biocatch

BIOCATCH Less Friction. Less Fraud.

SAMSUNG SAMSUNG SDS AMERICA