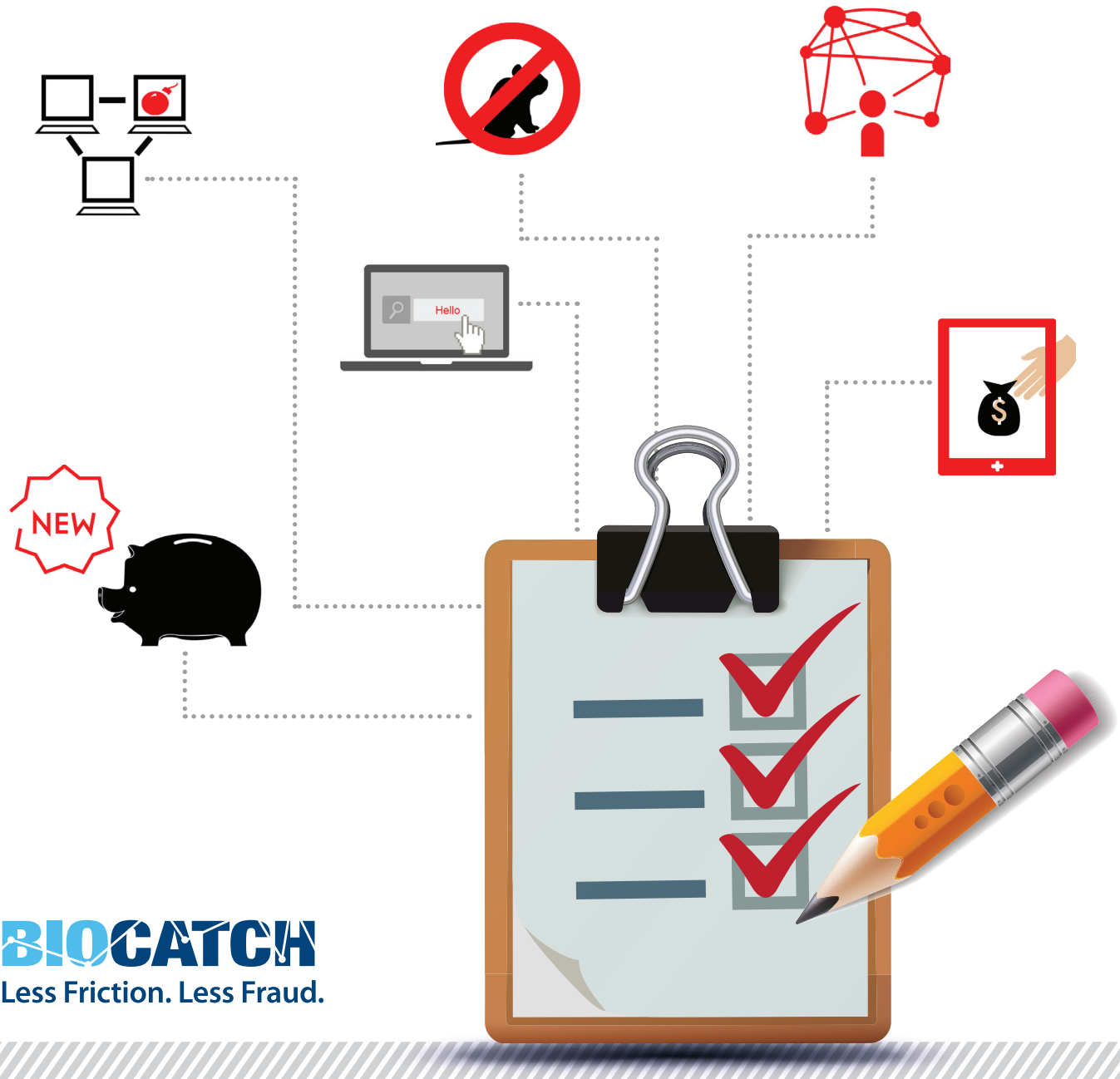
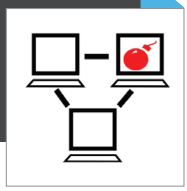
BioCatch Fraud Detection
CHECKLIST

6 Use Cases Solved with Behavioral Biometrics Technology



BIOCATCH
Less Friction. Less Fraud.

1 MAN-IN-THE- BROWSER MALWARE ATTACK DETECTION (E.G. DYRE, NEVERQUEST)



Challenge: Cybercriminals infect customers with financial malware that waits for a genuine user to login into an online banking site and then carries out fraudulent transactions automatically.

Solution: Unlike existing malware detection solutions that create alerts when a device becomes **infected,** BioCatch identifies the **actual attacks.** In addition, and unlike in existing solutions, BioCatch's approach works on ALL types and variants of malware and will not generate false alarms when an infected machine is not actually attacking (most cases).

Benefits:

- Detects most malware attacks
- No false alarms
- Not susceptible to evasion techniques

2 REMOTE ACCESS (RAT) DETECTION

Challenge: RATs provide cybercriminals with unlimited access to infected endpoints. Cybercriminals use RATs to access the online banking site via the user's genuine device. RAT functionality is a standard feature within financial malware and is becoming the weapon of choice for most fraud attacks – especially in commercial banking.

Solution: By analyzing a user's movement fluency and other behavioral attributes, BioCatch can detect remote access attacks.

Benefits:

- Detects 100% of Malicious RAT attacks in real time – such as DarkComet, Dyre, DriDex, ProRat, VNC and RDP Add-ons to Zeus and Citadel
- Very low false alerts

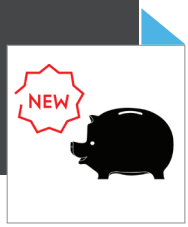
3 DETECTION OF BOT AND AGGREGATORS AT LOGIN

Challenge: Certain online banking login attempts are performed automatically by scripts. Fraudsters use botnets (a network of infected computers) to automatically login to accounts with stolen credentials in order to check their validity. Aggregators (such as Yodlee, MoneyCenter, Mint, and BillGaurd) use a similar mechanism to login and scrub account information (later presented through their apps). Naturally, banks have a vested interest in identifying both types of activities and distinguishing between them.

Solution: BioCatch's Behavioral Biometrics analyzes user login behavior to correctly identify between benign access (aggregators) and criminal access (botnets)

Benefits: Detect Bot attacks and aggregators to stop fraudulent access with stolen credentials.

4 NEW ACCOUNT SETUP (AND E- COMMERCE) FRAUD DETECTION

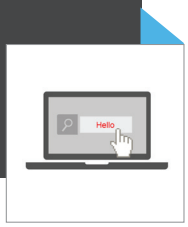


Challenge: Banks place greater emphasis on stronger authentication to prevent account takeover. Therefore, cybercriminals have started to shift their focus to the enrollment phase where fraud is committed by setting up online accounts using stolen/synthetic identity data. New account fraud typically occurs within 90 days following the opening of an account created with the sole intent to commit fraud.

Solution: BioCatch analyses the behavior of users throughout the application process and is able to distinguish between normal new account opening behavior and anomalous behavior by analyzing the following features: **user expertise, high application fluency and lack of data familiarity.**

Benefits: Reduce new account fraud

5 DETECTION OF ACCOUNT TAKEOVER FRAUD AT LOGIN/ TRANSACTION



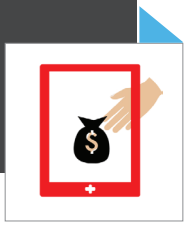
Challenge: Device spoofing techniques (e.g., FraudFox) and other evasion tactics are eroding the effectiveness of device fingerprinting solutions. Consequently, account takeover fraud is on the rise.

Solution: BioCatch can detect users that exhibit behavior consistent with known fraudsters or criminal behavior. Coupled with behavioral biometric authentication, BioCatch can detect many fraud attempts missed by current solutions.

Benefits:

- Reduces account takeover logins and fraudulent transactions
- Fewer alerts

6 ADD RISKY FEATURES TO MOBILE BANKING (ADD PAYEE, HIGHER TRANSFER AMOUNT)



Challenge: Bank customers are demanding more services on their mobile devices. Banks are struggling to add more functionality to their mobile apps in a usable way without taking on more risk. Asking a user to enter a username and password to approve a mobile transaction creates friction and is frowned upon by customer experience experts.

Solution: Banks can add BioCatch's behavioral authentication data to their risk engine, improving their risk scoring and mitigating risk to an acceptable level for new mobile functionality.

Benefits:

- Keeps banks at the forefront of the digital channel
- Enhances the customer's experience
- Shifts traffic from costly channels like branch and call center calls to the mobile app

BioCatch is a leading provider of Behavioral Biometric™, Authentication and Malware Detection solutions for mobile and web applications. Available as a cloud-based solution, BioCatch proactively collects and analyzes more than 500 cognitive parameters to generate a unique user profile. Banks and online & mobile stores use BioCatch to significantly reduce friction associated with risky transactions and protect users against cyber threats, such as Account Takeovers, Man-in-the-Browser (MitB) Malware and Remote Access (RAT) attacks. The Company was founded in 2011 by experts in neural science research, machine learning and cyber security and is currently deployed in leading banks across North America, Latin America and Europe. For more information, please visit www.biocatch.com

BIOCATCH
Less Friction. Less Fraud.

Contact us: info@biocatch.com
Follow us: Behavioral Biometrics Blog, LinkedIn, Twitter