

## Protecting Customer Data at Rest and in Motion

In terms of security threats, what we are seeing within our bank customers is a focused and increasing attack on online accounts. Phishing attacks, malware and other social engineering techniques are all on the rise and being used to steal access to online accounts. Indeed, the current financial services industry turmoil is creating many new opportunities for fraudsters to prey on consumers. These compromised online accounts are at the nexus of many different types of fraud. The fraudster will perform reconnaissance in the online account to simply look at information and then perform any number of other activities to accomplish the financial fraud:

- \* look at account balances and check images (to see MICR strip, check sequence number and signature block) and then execute counterfeit check fraud. There seems to be a rise in check fraud occurring in the industry.
- \* look at account balances and check images, then fax in a wire transfer request.
- \* look at account balances, personal contact information, recent transaction history and then call the call center to request a wire transfer, or change the address and request a new debit card, and so on.
- \* change the account address and request a new debit card via online banking application.
- \* use contact info, account numbers, and signature blocks to open an account in the victim's name in another financial institution. Then, establish an ACH connection between the two accounts and transfer money out of the victim's account and withdraw the money from the account they control either through the ATM or branch. Because the accounts share the same name, and because the fraudster can verify "ownership" of the victim's account (because they have credentials and can confirm the micro-deposit the ACH account registration process entails), the transfer is easy to pull off.
- \* use intra-bank money transfer feature of online banking to transfer money to a mule account (e.g., a victim of work-from-home scheme) at the same bank. The mule then extracts and transfers money from account.

These fraud schemes get categorized as check fraud or wire fraud and never get linked back to the original compromise. Indeed, most institutions have no easy means to make that correlation and the accounts remain vulnerable to further fraud.

In response to these threats, a layered security approach is most effective especially for online accounts. Most banks have implemented stronger authentication technologies, but in balancing security with customer convenience these implementations often have resulted in solutions that are relatively easy to compromise with today's fraudster techniques. Having a transparent, back-end fraud detection solution that complements authentication provides a more robust solution. Such a fraud solution should not be limited solely to analyzing transactions, but needs to look at all online activity to identify potential fraud.

Guardian Analytics FraudMAP® provides fraud detection, investigation and risk management capabilities for protecting online accounts from fraud and identity theft. Our approach protects accounts from login to logout and detects even the most benign-looking online account compromises allowing banks to stop fraud attempts before any loss occurs.



**Tom Miltonberger**  
CEO

**Tom Miltonberger** is President, CEO, Founder of Guardian Analytics. He has more than 20 years of executive and technology leadership experience. Prior to founding Guardian Analytics, Tom was the Senior VP of Products at Quova, where he led the development of groundbreaking IP Geolocation products and services. Tom is a recognized expert in using IP information for online fraud prevention, network security and regulatory compliance. Tom has held executive and leadership positions at Backflip, Decisive Technology, General Magic and Advanced Decision Systems. Tom received a BSEE and MSEE from the University of Illinois.



**Contact Info:**

<http://www.guardiananalytics.com>