

## Online Banking... Embraced by Customers - The Next Steps

While strides are being made to address online fraud detection, prevention and resolution, there are still huge industry gaps in terms of technology adoption of solutions that address all online touch points and user activities. Instead, many financial institutions have adopted either front-end solutions that aim to keep criminals from entering the online channel, or back-end fraud detection that tracks online activities in order to spot fraud. While those institutions that have deployed enhanced security measures are making great strides toward increasing confidence about using online services, the truth is a lot more can be done – both inside the bank and from a communications perspective – to break the online banking trust barriers that still exist in the market today and continue to hinder the adoption of Internet banking.

From an online banking perspective, banks that are leveraging technologies to “protect the front door” along with back-end fraud detection tools to continuously monitor the online channel are having the greatest success in truly addressing the increasingly sophisticated fraud tactics that are emerging on a more frequent basis. While nothing is full proof, banks that go the extra mile to protect all online touchpoints – from new accounts to online enrollment to login – and to track all user activities – from the moment a user accesses the Website until they logoff – need to truly convey to their current and prospective customers the fact that they are offering login-to-logout protection, in effect “chaperoning” their customers every time they visit the site.

Another key consideration beyond simply deploying security is to ensure that your bank has the tools to uncover what is happening in the online channel. After all, it’s hard to fight what you don’t understand. Any solutions deployed need to provide your organization with the ability to perform research, conduct analysis across the online channel, and deliver reports for compliance purposes and to ensure that all stakeholders within your organization have a clear picture of the risks within your online channel.

While imperative for understanding the weak spots within Internet banking, there are other benefits to advanced research and reporting tools as well – the ability to understand how your customers are utilizing your online channel, and to tailor service offerings to attract and retain customers. In particular, for younger consumers, they are very technology savvy and want access to relevant information – and quick. They demand that their online user experience is personal and to the point. Banks must address their specific needs, yet still be able to provide security without impacting their user experience.

At Digital Resolve, we have developed a solution suite that addresses the full fraud lifecycle by providing protection at the point of login and across all user activities and transactions – without impacting the user experience. By providing a first line of defense through our Fraud Analyst risk-based authentication platform and leveraging our Fraud Scan transaction monitoring and fraud detection solution, our clients are experiencing up to a 90 percent reduction in online fraud. Furthermore, our customers are discovering unmatched value in the insight they are gaining from our advanced research, analysis and reporting tools that allow them to take a deep dive into specific fraud incidents; access out-of-the box fraud reports; generate ad hoc queries; create compliance reports and audit trails; identify accounts linked to specific fraud incidents; schedule daily reports; and much more. Now clients have the ability to take a proactive role in fraud prevention, and are no longer waiting for customers to report fraud. Instead, we are empowering clients to reach out to customers – before they are affected by online crime.

Only by actively monitoring all activity online can your bank truly understand what is happening and have the ability to comprehensively address fraud. The more your organization understands about the true risks within your online banking applications, the easier it is to address those risks and communicate clearly with your customers about what your bank is doing to protect them.



**Dennis Maicon** is Executive Vice President of Financial Services Solutions at Digital Resolve. Dennis was a co-founder of Digital Envoy, and brings more than 18 years of financial services experience to Digital Resolve. Prior to joining Digital Envoy, Dennis was Senior Finance manager at Arris Interactive, where he was in charge of treasury functions, financial planning and analysis. Prior to Arris, Dennis spent nine years at Suntrust Bank where he held a variety of positions from credit administration to cash management functions to vice president of International Corporate Banking. Dennis holds an MBA from Georgia State University and an undergraduate degree from the University of Georgia in Finance.