



INTERVIEW TRANSCRIPT

# ACCOUNT TAKEOVER GOES MOBILE

Tim Dalglish of BioCatch on Fraud Trends, Behavioral Biometrics





**TIM DALGLEISH**

Head of presales engineering and professional services – APAC, BioCatch

“You need to go to the next level and look at how someone behaves on their device to pick up on account takeover fraud.”

The mobile channel saw great user adoption in 2020 – and it saw a corresponding increase in fraud incidents. Tim Dalglish of BioCatch talks about mobile fraud trends and the role of behavioral biometrics in enhancing user authentication.

In this video interview with Tom Field of Information Security Media Group, Dalglish discusses:

- Mobile adoption and fraud trends;
- Growth in account takeover;
- The expanding role of behavioral biometrics in authentication and fraud prevention.

Dalglish is a fraud prevention expert with over 15 years of experience. He has worked with businesses in over 20 countries to implement effective fraud prevention systems and strategies. At BioCatch, he is head of presales engineering and professional services – APAC. Prior to BioCatch, he led the APAC technical teams for both ThreatMetrix and RSA Security. Dalglish also spent 10 years at ANZ Bank and GE, leading various fraud prevention functions. He has spoken at many forums, including the Visa Risk Summit, RSA Conference and Money 20/20.


### **Growth of Mobile Adoption**

**TOM FIELD:** Looking back on 2020, what mobile adoption trends did you see globally? And how do regions compare to one another?

**TIM DALGLEISH:** We’ve seen volumes grow dramatically. We’ve gone from in the hundreds of millions of transactions, or sessions, per month to 1.5 billion per month on the mobile platform alone. Banks have traditionally been slow to adopt new technologies, but the mobile phone is now the bank branch. You need to be able to do everything by phone. You can deposit a check on your phone. It’s seamless, fantastic.

We do a lot of work in Latin America and the Asia-Pacific region. They’re mobile-first markets with high volumes. It’s probably three-quarters Android, one-quarter iPhone iOS in those regions. In North America, it’s closer to a 50/50 split.





“The game changer is that everything’s happening on the phone. People’s lives are on their phones.”

## Mobile Fraud Trends

**FIELD:** With this mass adoption, what trends are you seeing through the mobile channel?

**DALGLEISH:** Mobile malware really took off in 2020, primarily thanks to the Android ecosystem. It usually starts with some sort of social engineering. You get a text message on your phone with a link. If you hit the link, it installs an app. Then the malware owns the phone.

The phone is basically a little computer. So, once malware has ownership, it can do all sorts of crazy stuff –recording your calls, forwarding your calls, intercepting SMS messages, stealing people’s credentials, stealing one-time passcodes, taking remote control of someone’s phone. The malware is getting smarter. It can hide itself. There are lots of different strains.

We’ve also seen continual accelerated growth in social engineering. That’s when you get a phone call from someone trying to convince you to do something. The scam caller pretends to be from the government or a trusted brand and tricks you into doing something you wouldn’t normally do.

## Evolution of Account Takeover

**FIELD:** How has account takeover evolved via mobile?

**DALGLEISH:** The old-school fraud was, “I’ll use phishing to steal your credentials, log in from a new device and steal some money.” Now, it could be malware or taking remote control of your phone, which is common. It’s a cat-and-mouse game. I call you and trick

you into installing an app on your phone or a piece of malware that allows me to control your phone. But it appears that you are logging in from your normal phone, so it’s safe. The banking session is coming from the customer’s device, but the customer is not actually doing the session.

You need to go to the next level and look at how someone behaves on their device to pick up on account takeover fraud. To help explain how you can analyze behaviors, I hold my phone in my right hand and type fast with both thumbs. My father holds his phone in his left hand and types slowly with his index finger. We behave differently.

## Increase in Malware Attacks

**FIELD:** In 2021, mobile adoption is going to continue. People will continue to do e-commerce as we live within the pandemic. What coming account takeover trends concern you?

**DALGLEISH:** Malware attacks are going to increase. There will be more scams that involve taking over an account, with a criminal and a victim. I call them hybrid cases. It’s not that a bad guy logs in and steals money. There’s some customer involvement, too.

Open banking is going to play a part. It’s been slowly adopted and it’s potentially really useful to bad guys. It can be used as a proxy for committing fraud or managing fraudulent accounts through a third party.

“Behavioral biometrics gives you a competitive advantage. Behavior plays a really big part in empowering banks to protect their clients.”

## Beyond Traditional Authentication

**FIELD:** Authentication has never been more important than it is at this point in the history. Where do traditional authentication methods fall short, given the mobile fraud trends we’ve just discussed?

**DALGLEISH:** In a banking context, the customer experience of authentication might be an OTP SMS. That’s hard to implement and it’s even harder to change. If you have 5 million or 10 million customers, you’re not going to just throw it out. It’s a massive piece of work to migrate your customer base from one method of authentication to another. Traditional authentication is binary and hard to shift. You need an approach that is more flexible.

From a security perspective, if a criminal has control of your phone and the SMS OTP is coming to your phone, they suppress it so you can’t see it and it gets forwarded to the criminal. The authentication is going to the customer’s phone, but then it’s getting bounced to the criminal. You need to think about authentication in a different way when you’re trying to manage the risk alongside the customer experience.

The game changer is that everything’s happening on the phone. It’s where the customer is doing the banking, and it’s where the authentication is happening. People’s lives are on their phones.

## Behavioral Biometrics

**FIELD:** What is the growing role of behavioral biometrics?

**DALGLEISH:** Behavioral biometrics is about collecting data, manufacturing data and drawing insights. It gives you flexibility because it’s not binary. Traditional authentication is “yes” or “no.” But collecting lots of data gives you insights around a whole lot of things and can help you make a better decision.

Behavioral biometrics gives you a competitive advantage. Behavior plays a really big part in empowering banks to protect their clients, because the fraud is coming from the customer’s device or the customer is being tricked into doing something they wouldn’t normally do. Knowing the customer’s typical behavior can help detect the fraud.

The fraud controls that are effective are ones that cannot be easily reverse-engineered by the criminal. If you’re collecting loads of data and you’ve got complex algorithms, and you know the customers and how they behave really, really well, then it’s basically impossible to reverse-engineer from a criminal perspective. ■

---

Listen to the full interview: <https://www.inforisktoday.com/account-takeover-goes-mobile-a-15832>

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • [sales@ismg.io](mailto:sales@ismg.io)

 **BANK INFO SECURITY®**

 **CU INFO SECURITY®**  
Just for Credit Unions



 **GOV INFO SECURITY®**



**HEALTHCARE INFO SECURITY®**

 **infoRisk**  
TODAY



**CAREERS INFO SECURITY®**

**Data Breach.**  
Prevention, Response, Notification. TODAY

**CyberEd.io**

  
**ISMG**  
INFORMATION SECURITY  
MEDIA GROUP