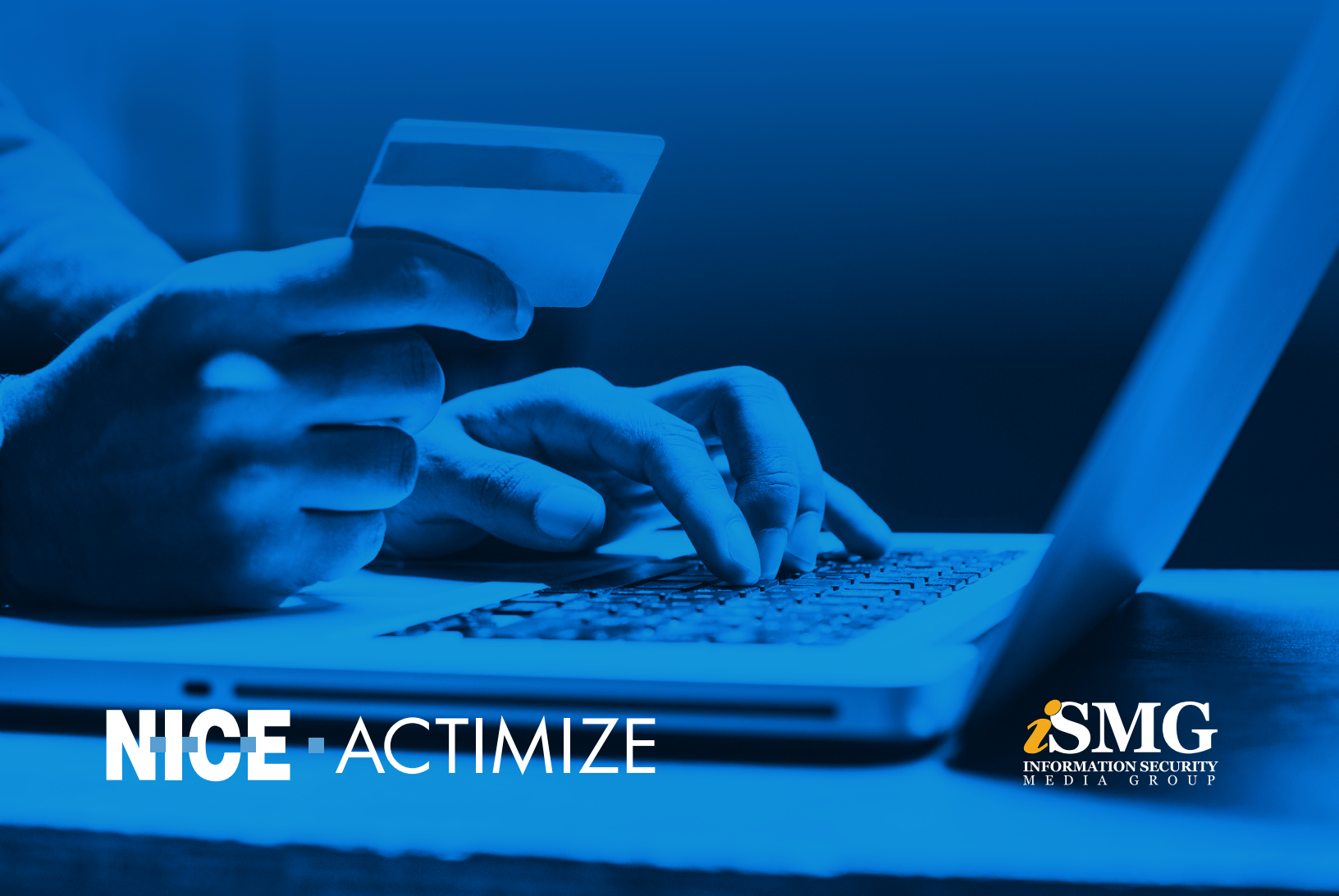
# Defending Against Authorised Push Payment Fraud

Rob Tharle of NICE Actimize on How Banks Can Help Protect Their Customers



NICE · ACTIMIZE

ISMG INFORMATION SECURITY MEDIA GROUP

NICE · ACTIMIZE


A Fraud and Authentication Subject Matter Expert, NICE Actimize EMEA, Tharle, is responsible for providing thought leadership on industry trends, challenges and opportunities. Prior to joining NICE Actimize in 2019, he worked for 17 years in a number of Risk Management and Fraud Prevention roles at both Natwest/RBS and TSB. During that time, Rob gained extensive experience with the technologies and design of fraud prevention and detection systems including application fraud, Apple and Google Pay, online and mobile banking.

The advent of faster payments has helped accelerate authorized push payment fraud schemes in which victims are defrauded under false pretenses. Banking regulators are responding to the trend, and Rob Tharle of NICE Actimize offers advice for multilayered defense.

Tharle, a Fraud and Authentication Subject Matter Expert with NICE Actimize EMEA, says authorized push payment fraud is dramatically different from many other forms of fraud banks face.

"[With APP fraud], the customer has authorized the payment, as opposed to a fraudster authorizing it, and that means that under most laws the consumer is liable for it," Tharle says, adding "The sums of money are very large and life-changing."

In an interview about APP fraud, Tharle discusses:

- Why APP fraud incidents are rising;
- How regulators have responded;
- Multilayered defensive tactics.

## Push Payment Fraud

**TOM FIELD:** Rob, let's talk about authorized push payment fraud, the challenge it presents and why this is getting noticed now in particular.

**ROB THARLE:** It's a really interesting space, and it's getting noticed really heavily in the U.K., but some of the other jurisdictions as well, including the U.S. and the Nordics. And the reason is the really large amount of money that customers are losing and the potentially life-changing consequences to them.

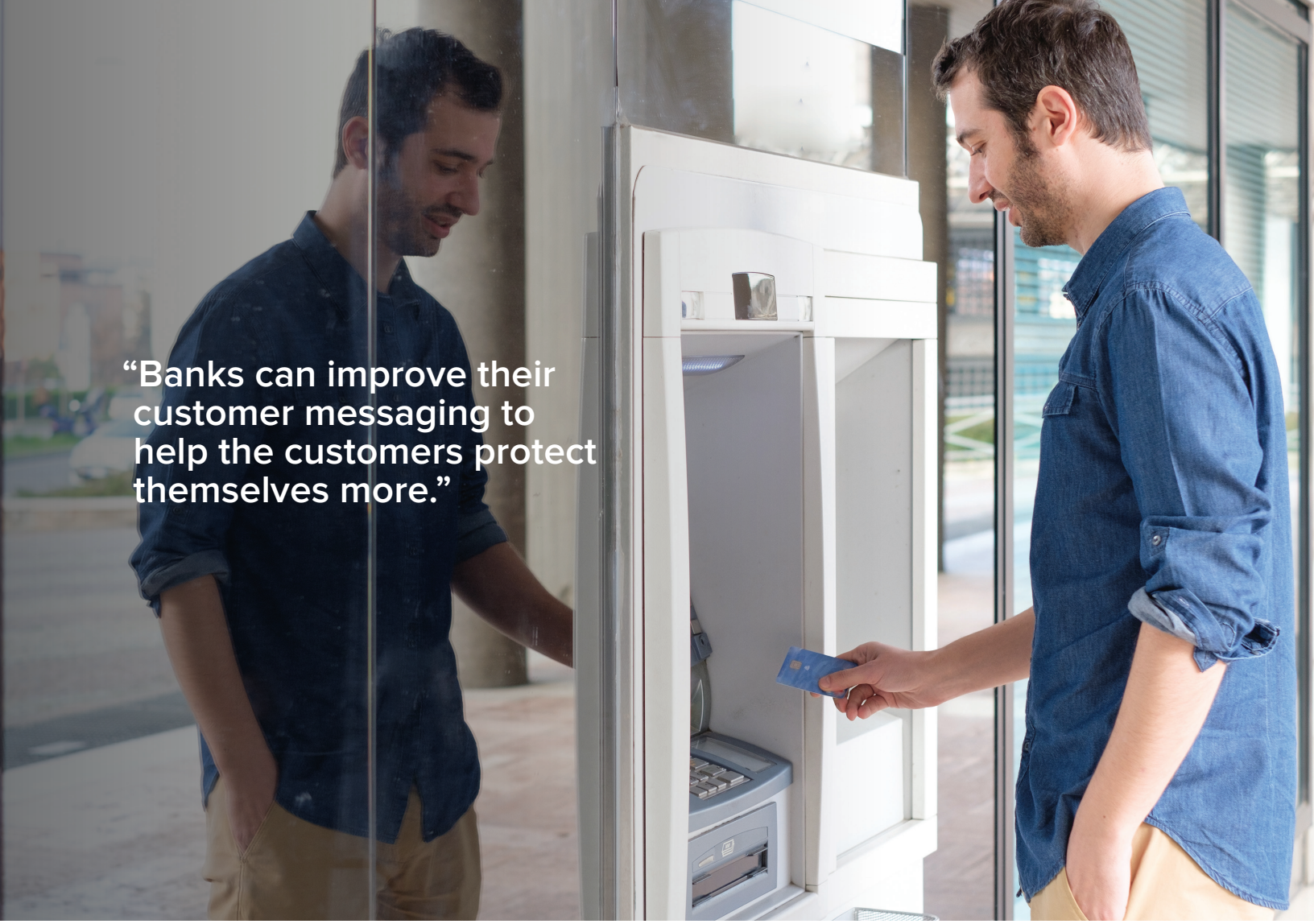
The regulators are really picking up on that and want the financial industry to do something to help those consumers out.

## Regulators Respond

**FIELD:** Well, to follow up on that Rob, how have regulators responded to this trend that you've seen?

**THARLE:** The U.K. regulators, particularly the payment services regulator and the FCA, are focusing in on protecting the consumer and making sure they get refunded. Authorized push payment fraud differs from the normal type of fraud we're used to – account takeover fraud – in that the customer has authorized that payment as opposed to a fraudster authorizing it. And that means that under most laws, the consumer is liable for it and the bank doesn't have liability. And so they don't get refunded, and the types of fraud that are involved – romance scams, investment scams or business email compromise payment frauds – mean that the sums of money involved are very large, and, as I've said, life-changing.

The U.K. regulators have just had the U.K. banks voluntarily agree to implement something called the contingent reimbursement model, and this means that they will reimburse these customers in certain circumstances if they've been a victim of push payment fraud.




## Defensive Tactics

**FIELD:** So Rob, in terms of security controls, what types of multilayered defensive tactics do you recommend that institutions adopt?

**THARLE:** Well, there are a number of actions, and these particularly align with the contingent reimbursement model. But the key ones are looking to protect customers both outbound and inbound, as the receiving bank and the paying bank. They can improve their customer messaging to help the customers protect themselves more.

So, it includes education campaigns and then also, very specifically within various payment journeys, putting up risk-based warnings to them that something might be amiss and trying to trigger that important response in a customer to think rationally and ask: “Does this make sense?” Because most of the time, these things don’t make sense, and the fraudster has instilled a sense of urgency and/or fear to bypass their rational thought processes.

Then also, use all the digital tools they’ve got available to them – device profiling, behavior biometrics, malware detection – and layer that with a good fraud platform and advanced analytics so that they can build specific models to identify customers who are at risk of these sorts of fraud and the payments themselves – and indeed, accounts receiving those payments.

Beneficiary banks in the past have not had the right incentives to invest properly in this space – to undertake real-time profiling of inbound payments and freeze those where required. And pulling all those things together with a really good case management system that can allow banks to look at the entities involved, highlight unusual behaviors and network links as well, means they can identify all these sorts of fraud in an efficient way, only really impacting the fraudsters and not the genuine customers going about their business.

## Business Benefits

**FIELD:** Well, beyond stopping fraud, it strikes me there could be some business benefits realized from these defensive tactics as well, would you agree?

**THARLE:** Definitely. And that’s really where there are some good things to happen. Banks who choose to invest in the right systems and take the right approach to this – protecting customers and building out their business – will get those rewards, protecting

customers from these frauds and scams as well as impacting their bottom line of reducing their liabilities and their fraud losses. It will also create a hostile environment for the fraudsters, reducing further the costs on their business. It will also reduce management time they're spending dealing with the regulators on these matters. But it also helps support putting trust back into the system.

So with all the new innovations coming down the pipe, whether that's through open banking or voice-first with the payments via Alexa … customers will then have trust. It gives those organizations a head start over everyone else in reaping those benefits.

> "Banks who choose to use all the digital tools available, layered with a good fraud platform and advanced analytics, can build specific models to identify customers who are at risk of these sorts of fraud."

## NICE Actimize's Role

**FIELD:** Rob, final question for you. Talk to me a bit about NICE Actimize. What are you doing to bring this to your customers' attention and assist them in putting up an appropriate defense?

**THARLE:** We can provide the sorts of systems that allow customers to do this, both with out-of-the-box models and also advanced analytics, working with those customers to build the sorts of profiles they need to do all of the things I talked about earlier.

That can be purely on the paying away side or, indeed, on the inbound payments side as well. It involves building a platform and a hub for customers to put all their data in and make good quality decisions in real time to protect their customers and their own P&L as well, and doing that in an efficient way so that they're not having an army of people work all the alerts that are generated, but doing that in a cost-effective fashion. ■

## 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.

## Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io