The Route to Trusted IDs

New Strategies for Fighting Fraud with Equifax's John Marsden

ISMG INFORMATION SECURITY MEDIA GROUP

EQUIFAX®

When it comes to describing the top fraud threats to U.K. financial institutions, it's all about compromised identities and credentials, says **John Marsden** of Equifax. How can organizations prove their customers are who they say they are?

Identity is *the* hot topic, says Marsden, Head of ID and Fraud-Decision Strategy, for Equifax Europe.

"In the U.K. identity fraud is the highest level of threat we're seeing, and that encompasses compromised identity, synthetic identity and ID takeover attempts. That's borne out by national figures," Marsden says.

Also undeniable is how customers demand fast, responsive service. And they don't have patience for anti-fraud controls that in any way impede the customer experience.

"In a digital environment, good customers deserve to be served quickly. If they aren't, they walk away," Marsden says. "Your business relies on being able to spot the good customer and accept the bad customer at pace and speed using a lot of different layers of intelligence to be able to give you those insights you can act upon."

In an interview about fighting fraud by authenticating identities, Marsden discusses:

- Why traditional anti-fraud tools are ineffective against today's top schemes;
- How organizations can prove that customers are really who they say they are;
- How to enhance security without hurting the customer experience.

John Marsden is Head of ID and Fraud-Decision Strategy at Equifax Europe. In this role he is responsible for the overall development of the Equifax U.K. ID and Fraud business, involving various initiatives from client representation to developing partnerships and contributing towards product development, marketing and PR initiatives.

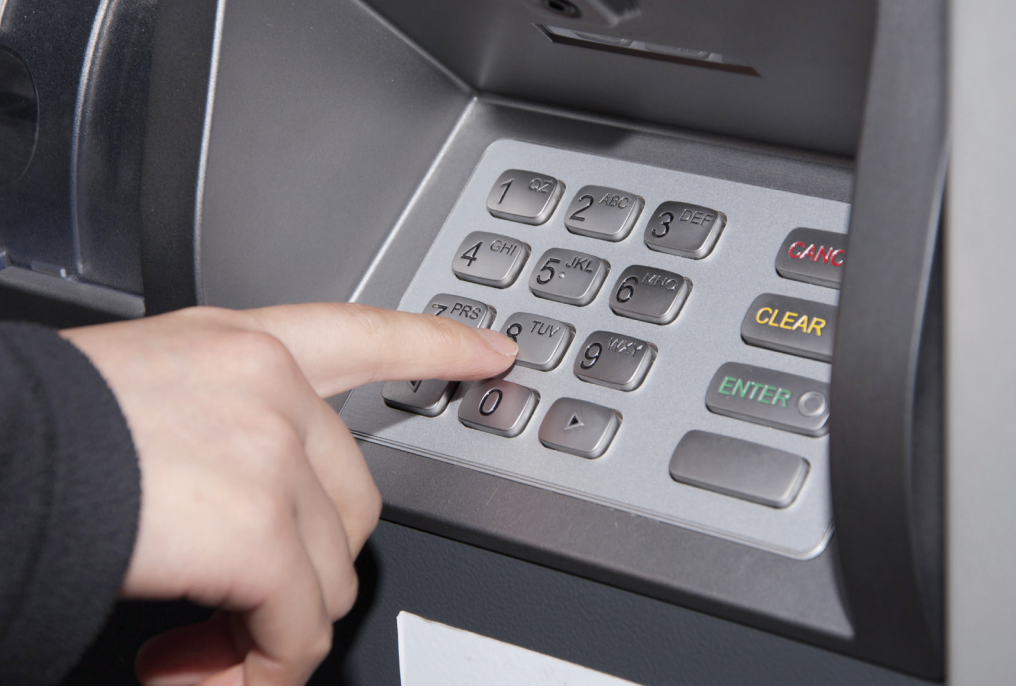
John Marsden

Main Fraud Threats

TOM FIELD: John, give me some perspective. What are some of the main fraud threats that organizations struggle with today?

JOHN MARSDEN: From our perspective and our clients' perspectives it's very much about identity, and that comes in a multitude of different ways. In the U.K. identity fraud is the highest level of threat we're seeing, and that encompasses compromised identity, synthetic identity and ID takeover attempts. That's borne out by national figures.

FIELD: How do you see fraud impacting businesses themselves as well as the general public?



MARSDEN: Fraud is a huge challenge for businesses. In a digital environment, good customers deserve to be served quickly. If they aren't, they walk away. Your business relies on being able to spot the good customer and accept the bad customer at pace and speed using a lot of different layers of intelligence to be able to give you those insights you can act upon.

> "In the U.K. we have ample data to prove a person exists. ... But proving a person is who they say they are is more of a challenge."

How MLD4 Affects UK Lenders

FIELD: John, how does MLD4 (Fourth Money Laundering Directive) specially affect U.K. lenders?

MARSDEN: The money laundering directives have been with us for a while with the clear objective of stopping terrorist financing and the laundering of the proceeds of crime. MLD4 changes the ability for domestic lenders to ignore their own past, for example, and that's a big thing. A politically exposed person is susceptible to corruption, and previous to MLD4 you could ignore the U.K. politicians, their relatives and close associates. Now you can't, and if you can imagine how many politicians we have in the U.K. down at the city level, along with their relatives and close associates, then we have to step up our authentication of those people.

In addition, we have to practice enhanced due diligence to ensure we know where their funds come from. That's probably one of the biggest challenges of MLD4. MLD4 is an extension of what was there before, but it does need that rigor to apply those measures instantly in a digital environment without causing too much friction for a Joe Blow who just happens to share the same name as a wife or a husband of a politician.

Why Traditional Fraud Tools No Longer Work

FIELD: From your perspective why are traditional anti-fraud tools and techniques now ineffective against many of the schemes that you're seeing?

MARSDEN: That's focusing on identity fraud, and I think there is a real key difference that I can see across our worldwide spread at Equifax. The U.K. has been very effective at sharing and syndicating fraud knowledge. When an identity is used for fraud, it gets logged with [U.K. fraud and cybersecurity prevention non-profit organization and confirmed fraud database] Cifas and with available commercial products to screen those identities.

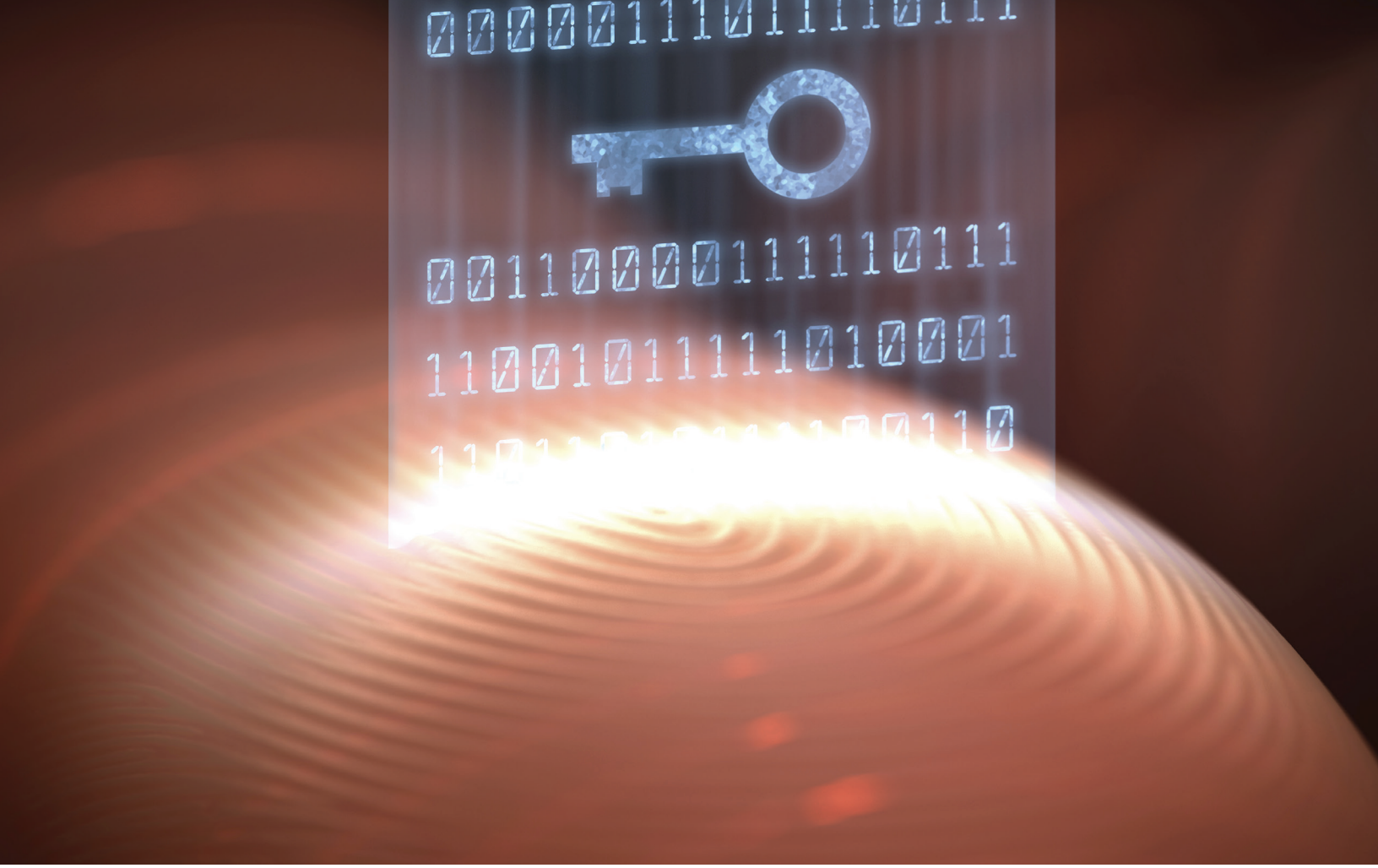
The fraudsters know this, and as a result, they attempt an ID takeover within two or three days, and then leave that identity alone. Why is that? After that time period, that stolen identity is logged with Cifas and some of the commercial agencies that share this information, including Verisign, and we block the use of that identity for the fraudster, who has massive amounts of data available to them that is still perceived as clean, which lets them move to the next case and the next one.

Unfortunately, that's not common across the rest of the world, where there is a lack of fraud exchanges like Cifas. So, for example, in the U.S. an ID takeover can last three, four or five months, as fraudsters use that identity over and over. Now assume that is tightened down with the use of fraud technology, but when you face an environment like the U.K.'s, where you have to spot that fraud in that two-day window when the ID takeover is happening, you do need new technology, new layers and new intelligence to lead you to spot that fraud amongst the other applicants.

The Fundamental Challenge of Identity

FIELD: John, let's talk about this identity challenge because I've heard organizations around the world talk about this same challenge. How do you see organizations proving that their customers really are who they say they are and live where they say they live?

MARSDEN: In the U.K. we have ample data to prove a person exists. We can measure the length and breadth of the identity within a household. But proving a person is who they say they are is more of a challenge. Traditionally, we've relied on knowledge-based authentication, which concludes that you're authenticated if you have the knowledge of that person. And fraudsters have adapted to that. We still use KBA, but it no longer is the be-all-and-end-all.



> "We're not yet at a place of being able to share biometrics on the general population, so we have to use multiple layers of intelligence to spot a risk."

We're not yet at a place of being able to share biometrics on the general population, so we have to use multiple layers of intelligence to spot a risk. That may be at the device or SDID layer and all the intelligence gathered from the velocity usage of a given identity. The end of that process might end up in a document and facial verification of the individual to really prove they are who they say they are.

But you can't do this all the time because that causes too much friction for the U.K. consumer, who are not used to carrying their passports around with them. So, it has to be measured in its approach. You have to use the intelligence you get from multiple layers to determine when it's appropriate to take a customer through a frictional experience and when it's not.

The Need for Multifactor Authentication

FIELD: You're on to a good point there, John, because certainly organizations worldwide share this same challenge, although I can't say a lot of them are taking significant steps to do anything about it. So, why have solutions such as multifactor authentication for instance been relatively slow to take hold, even though organizations all see the same problems?

MARSDEN: You need two-factor authentication. The problem, primarily in the applications space, is that you haven't got the ability to use a second factor and authenticate its second factor until you bothered that client and involved them in such a service. That's one of the challenges for the application space in login, account maintenance and account monitoring terms. How do you challenge someone to be who they say they are when we don't record the second factor? That could be a facial biometric or how the customer uses their machine. So, that's a challenge.

You should be enrolling people in two-factor authentication. The importance of that is seen adamantly in the Yahoo breach. Once you've started breaching passwords at the rate we have and have the computing power to turn them into real metrics, then no password is safe.

"One of the big things we're seeing across our customer base is the adoption of device recognition and reputation."

How Equifax Helps Fight Fraud

FIELD: John, talk to me about Equifax. What are you doing to help your clients fight fraud differently and better?

MARSDEN: We, at Equifax, have a lot of data, and we're going through this transformation of turning all that data into great insights for our customers. The precision and recall rates we're achieving are exceptional and beating traditional systems. We're using machine learning to leverage that data and provide our customers with real intelligence that helps them manage the issues they come across in the fraud environment.

FIELD: What are some of the results that your customers are seeing through using your solutions?

MARSDEN: We're seeing a reduction in false positive rates by using these multiple layers of intelligence. And what does a false positive rate mean? It generally means a lost customer. So, we're seeing more clients able to be boarded more seamlessly and more in the way they want to be boarded. Also, we're seeing more precision in the exception effort going in. It's intangible, but you're looking at using those multiple layers. Taking precision down from one-to-three ratio towards a one-to-one.

Reducing Friction

FIELD: Final question for you John. You talked a few moments ago about friction in the process. How can organizations implement more security controls without introducing that friction and without damaging the relationship with their real customers?

JOHNSON: It's a balancing act. One of the big things we're seeing across our customer base is the adoption of device recognition and reputation. In the early days we saw this adoption through the more fast-moving industries, such as in gaming and short-term loans. That has now transferred to our more blue-chip clients that previously lacked this level of intelligence because they were skeptical about what it could do for them.

This is a great example of where you can deploy something that's silent to the consumer, but gives you a deep level of understanding about that interaction with that consumer and about that application. That is essentially the base layer now for our Progressive Authentication suite and the key identifier that informs the rest of the challenges we make to either ratchet up the friction or turn down the friction in a dynamic approach to fraud protection and prevention. ■

http://www.bankinfosecurity.co.uk/interviews/route-to-trusted-ids-i-3348

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401
sales@ismgcorp.com

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

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

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com