3rd Annual Financial Services Cyber Security Summit

Wednesday 13th July 2016

Peter Oakes, Fintech Ireland / Fintech UK

Peter Oakes

- Executive and non-executive director and advisory committee member to regulated and unregulated companies, including Fintech, RegTech, MiFID and Funds. Panel Member, Fintech20 Ireland
- Solicitor admitted in Ireland, the United Kingdom and Australia
- Founder of Fintech Ireland & Fintech UK (RegTech Ireland & Regtech UK). These groups support ‘fintech’ & ‘regtech’ initiatives in Ireland & the UK
- 2014-2016: Board Director & Chief Risk Officer for Bank of America Merchant Services Europe (based in London)
- 2010-2013: Central Bank’s first Director of Enforcement and AML/CTF Supervision in October 2010. Member of the Senior Leadership, Operations, Policy & Supervisory Risk Committees
- Over the past 25 years Peter has worked as a regulator (Ireland, UK & Australia) and in the investment management, payments, funds & fintech industries (UK & Ireland) in Board, C-Suite, Legal and Compliance/Risk roles. He has also advised Central Banks, Regulators and their senior management on a wide range of supervisory and enforcement issues

FinTech & RegTech – cyber security

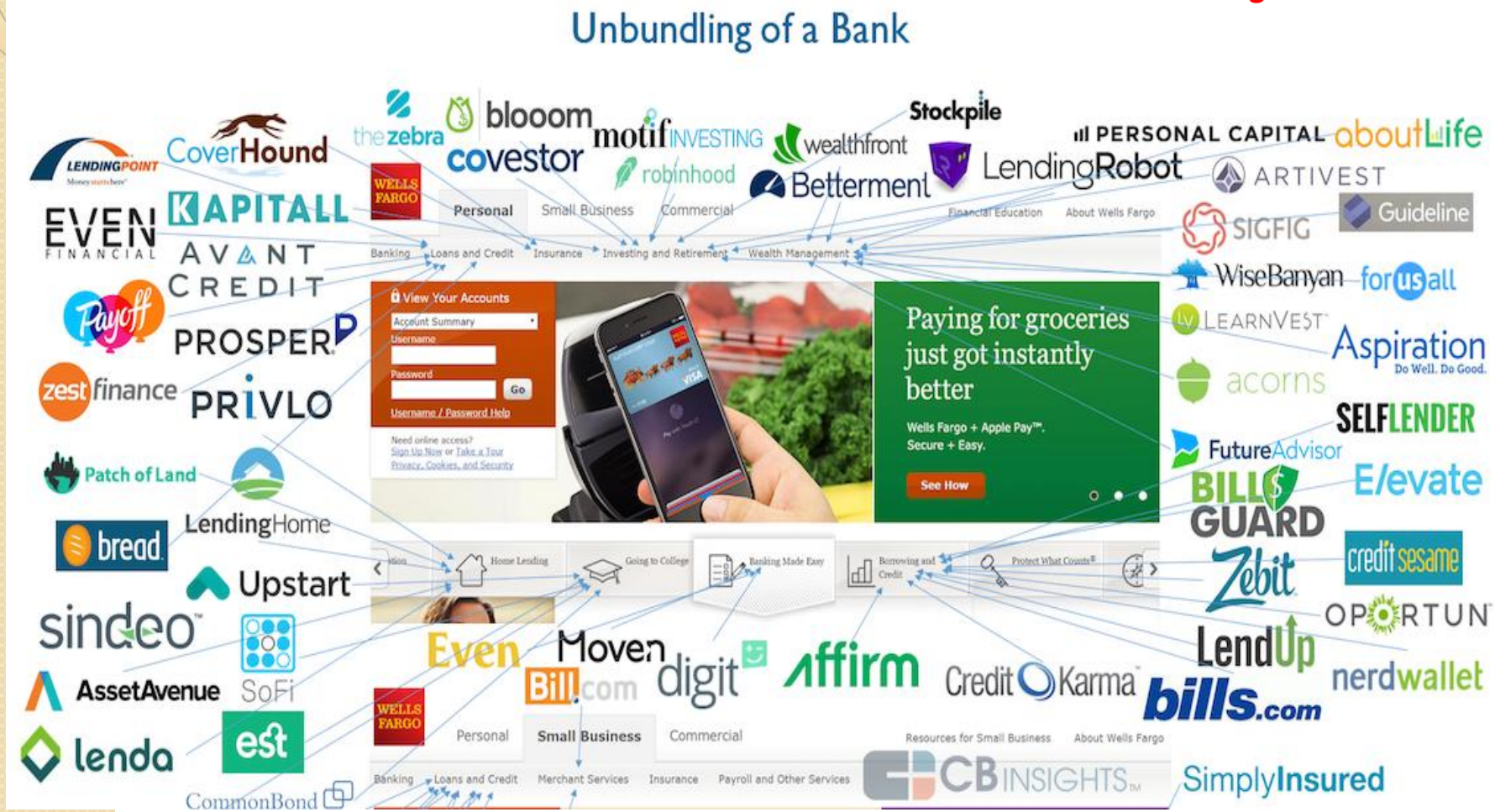
Case Study II

How will Fintech & RegTech drive cyber security? Future scenarios and possible solutions

Peter Oakes, *Founder and Fintech Member, Fintech Ireland*

Unbundling Banks

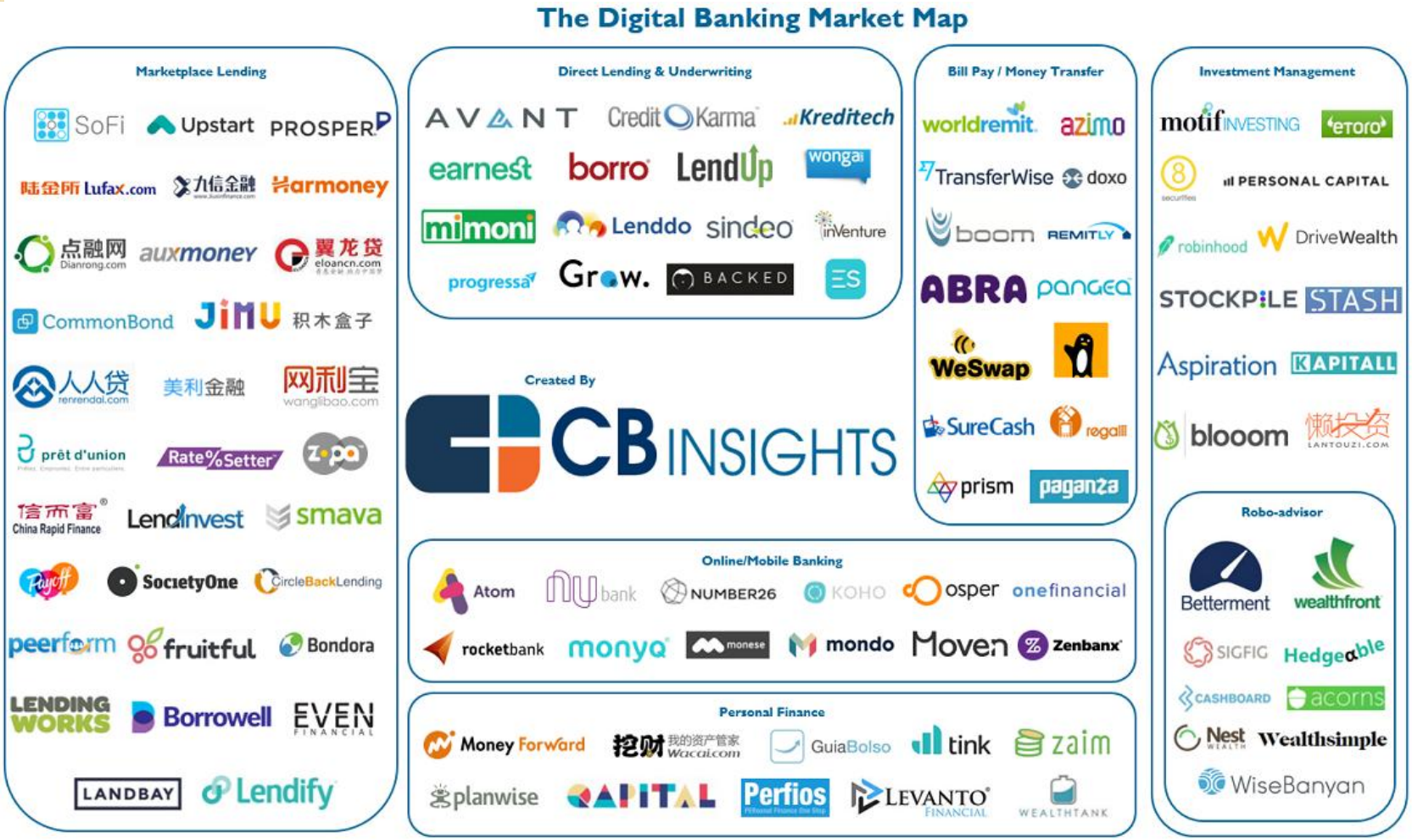
Source: © CB Insights



Fintech Attacking Banks' Value Chain

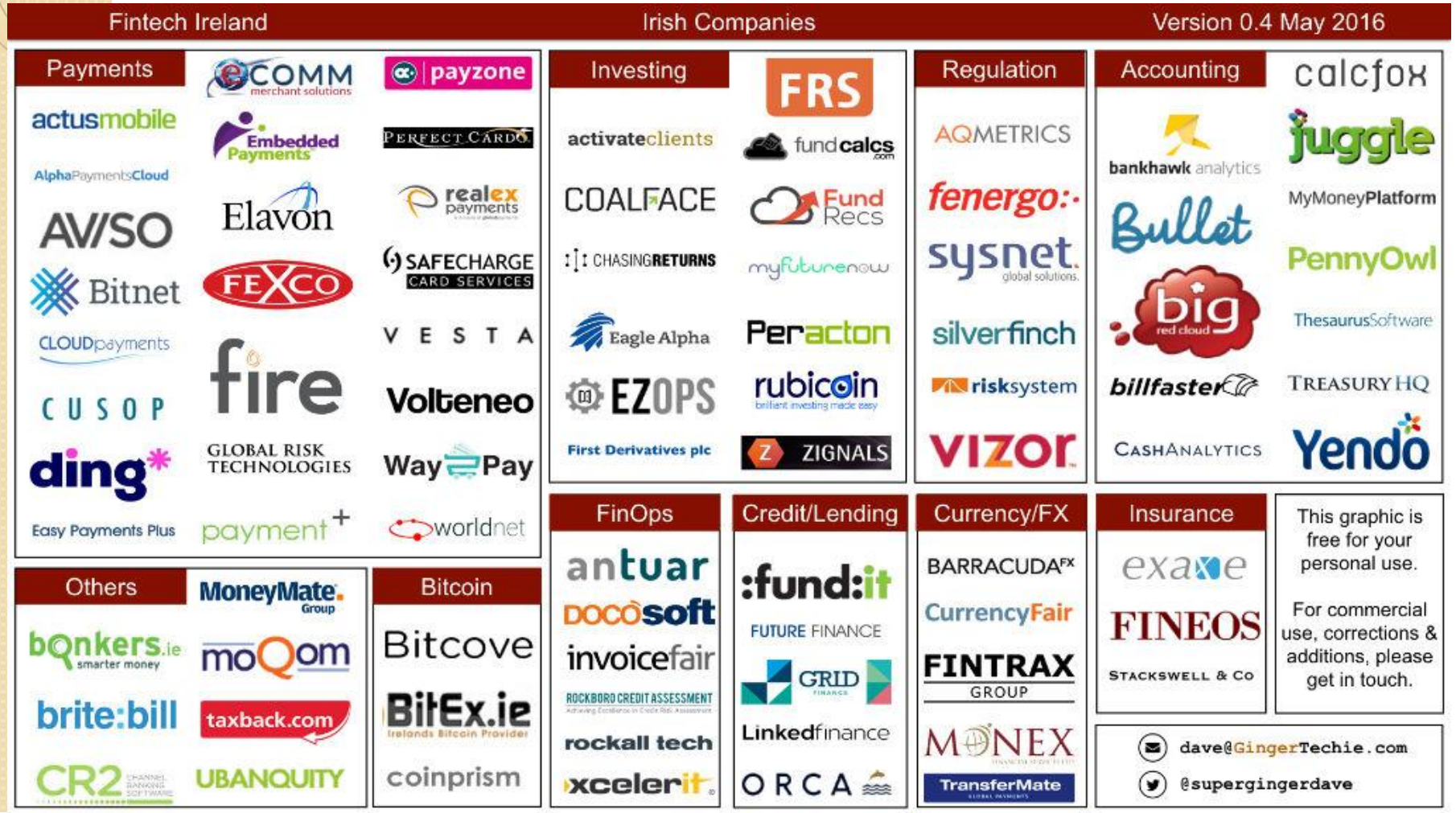
fintech IRELAND

Source: © CB Insights



Ireland's Fintech Ecosystem

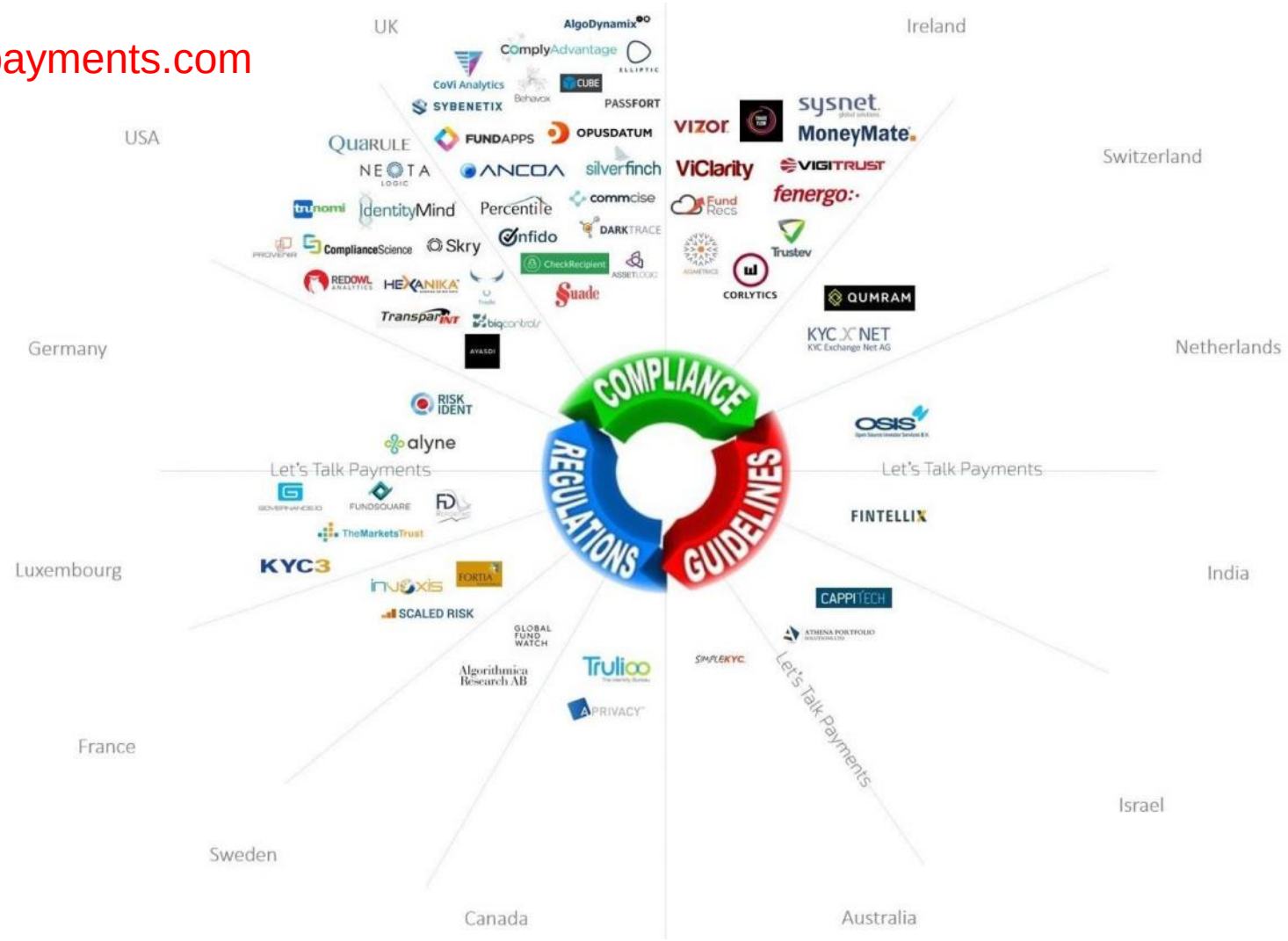
Source: © Dave Anderson / https://www.linkedin.com/in/daveandersonireland



fintech IRELAND

A Global RegTech Map

www.letstalkpayments.com



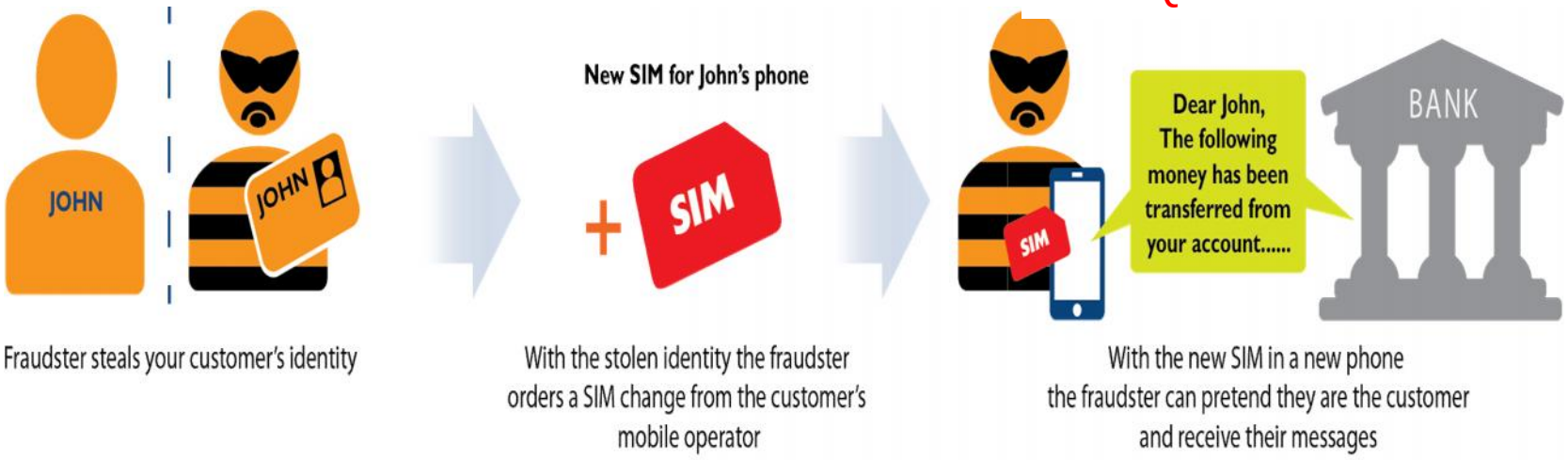
SIM Swap – What is it?

- SIM Swap is a basic functionality made available by Mobile Operators
- You have probably done it
- Allows customers to
  - move their mobile number from one network to another
  - change SIM card formats when changing make / model of their phone
  - recover their phone number if its lost or stolen.

What is a SIM Swap Attack? - 1/2

SIM Swap Explained

How a SIM Swap Attack Occurs



Fraudster steals your customer's identity

With the stolen identity the fraudster orders a SIM change from the customer's mobile operator

With the new SIM in a new phone the fraudster can pretend they are the customer and receive their messages

What is a SIM Swap Attack? - 2/2

- A SIM Swap attack occurs when a fraudster tricks the Mobile Operator into believing they are the legitimate owner of the mobile number, for example through social engineering
- Fraudster simply convinces a shop worker to provide them a new SIM card with the targets telephone number on it
- All the fraudster needs is a believable story regarding the fate of the lost, stolen or broken handset, a stolen/fake utility bill for the address of the target, and the target's mobile phone number
- By doing so, the Mobile Operator unknowingly transfers the victim's mobile number onto a SIM card in the fraudster's possession, which when placed in a new handset, allows the fraudster to gain access to the victims banking services

SIM Swap Fraud

- United Kingdom
- Ireland
- Australia
- South Africa
- Abu Dhabi

United Kingdom

Two major high street banks will change security procedures after journalists from BBC Radio 4's You and Yours programme broke into an account online and removed money.

Recently bank customers accounts have been successfully attacked by criminals who divert mobile phone accounts.

By Shari Vahl
Reporter, You and Yours

Criminals persuade phone providers to divert mobile phone numbers in what is sometimes called "SIM swap fraud".

theguardian

Sim-swap fraud claims another mobile banking victim

Chris Sims' account emptied and loan for £8,000 taken out as fraudsters continue to exploit way banks use customers' mobiles

Miles Brignall

Saturday 16 April 2016 07.00 BST

Ireland

Are banks answering the call on mobile phone security

Reliance on mobile phones for online payments could leave us vulnerable

about an hour ago

Ciara O'Brien Follow @ciaraobrien

Mobile phones have become an integral part of our lives, replacing everything from face-to-face interaction to good old maps as they become increasingly powerful. They are the hub of social lives through Facebook and other social networks, chat apps and email. They are work tools, creative hubs, entertainment, research and payments, all in one handy device.

In recent months, your mobile phone has become a digital wallet of sorts, allowing you to make payments online or in shops without having to physically have a card or cash on you.

moQom

http://www.irishtimes.com/business/technology/are-banks-answering-the-call-on-mobile-phone-security-1.2704035

THE IRISH TIMES

Recent report on SIM Swap fraud

SIM SWAP EXPOSURE IN IRISH RETAIL BANKS SUMMARY

Dated: 31st May 2016

Introduction

SIM Swap fraud has been an issue across the globe for a number of years. However, it wasn't until journalists on BBC Radio 4's 'You and Yours' demonstrated how easy it is to hack a bank account, that the scale of the problem became apparent.

In light of this, the Irish Times in consultation with the moQom sought to investigate and understand the level of exposure to such an attack in Ireland's most prominent retail banks. This brief report highlights some of the key findings of the research.

A more detailed explanation of the research process and its findings can be provided upon request and under Non-Disclosure Agreement. In such circumstances, please contact contactus@moqom.com

What is a SIM Swap Attack?

SIM Swap is a basic functionality made available by Mobile Operators so that customers can: move their mobile number from one network to another, change SIM card formats if they change the make and/or model of their phone, and recover their phone number if their phone is lost or stolen.

A SIM Swap attack occurs when a fraudster tricks the Mobile Operator into believing they are the legitimate owner of the mobile number, for example through social engineering. A fraudster simply convinces a shop worker to provide them a new SIM card with the targets telephone number on it. All the fraudster needs is a believable story regarding the fate of the lost, stolen or broken handset, a stolen/fake utility bill for the address of the target, and the targets mobile phone number. By doing so, the Mobile Operator unknowingly transfers the victim's mobile number onto a SIM card in the fraudsters' possession, which when placed in a new handset, allows the fraudster to gain access to the victims banking services.

Terms of Reference

The purpose of the research conducted was to assess, in an unbiased and objective manner, whether Irish banks were exposed to a SIM Swap attack and identify, based on the information available through their terms and conditions, who is held liable in the event of such an attack.

Based on the findings, the report was also tasked with providing hypothetical scenarios to illustrate, just what impact a SIM Swap attack might have on a bank customer in terms of financial loss and liability, in a comprehensive and easy to understand manner.

Methodology

The report focuses on banks whose processes rely on the customer mobile number as a security device, identifying any SIM Swap related weaknesses and verifying the level of protection offered to Irish customers by Irish banks.

www.moqom.com

- What is a SIM Swap Attack?
- Terms of Reference
- Methodology
- Key Findings
- Consumer Exposure
- Broader Implications

Australia

ID theft in three steps: 'Adequate' Telstra and telco identity checks questioned

Share SHARE TWEET MORE

July 9 2016

Esther Han

Follow

HUFFPOST AUSTRALIA

Tesla's Nightmare Month Just Keeps ...

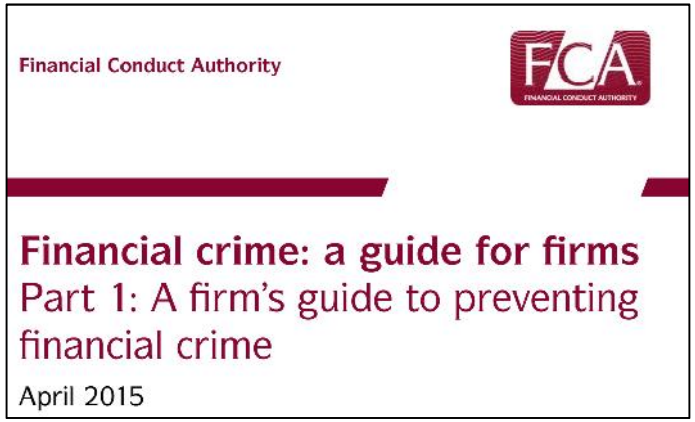
"All that person needed was my full name, date of birth and home address to get into my inbox and I'm concerned it's just too easy," said Ms King, a teacher from Lilyfield.

Cyber Security – Regulatory Expectations

- Irish and UK cyber security governance initiatives
  - *there are other regulators that are focussing on this area, e.g. EBA, IOSCO, ASIC, SEC and pretty much every EU regulator*
- The role of the Board
- The accountability of the Non-Executive Director (NED)
- The relationship between the CRO / CSIO, the Board and the NED

Data Security & Cyber Security - Financial Crime

- FCA refers regulated firms to examples of good and poor practice in data security at Chapter 5 in Part 1 and Chapters 6 and 10 in Part 2 of our Financial Crime: A Guide for Firms
- "Outsourcing to a 3rd party does not mean you have outsourced your obligations to look after customer data. [Must] carry out due diligence on 3rd party suppliers before hiring them, try to establish what their vetting procedures are, and ensure that they respect your firm's security arrangements"
- If you are a senior manager or board director of a FCA regulated entity take note



Is it really a matter for the Board? YES!

- See Central Bank letter on operational risk & cyber security dated 22 September 2015

"It is the responsibility of the board to ensure that a firm is properly governed"

Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

T +353 1 224 6000 F +353 1 671 6561

Cáirt Uibh Eachach, Bloc D, Bóthar Fhearchair,
Baile Átha Cliath 2, Éire.
Iveagh Court, Block D, Harcourt Road, Dublin 2, Ireland.

www.centralbank.ie

22 September 2015

Review of the management of operational risk around cyber-security within the Investment Firm and Fund Services Industry

Dear Chair,

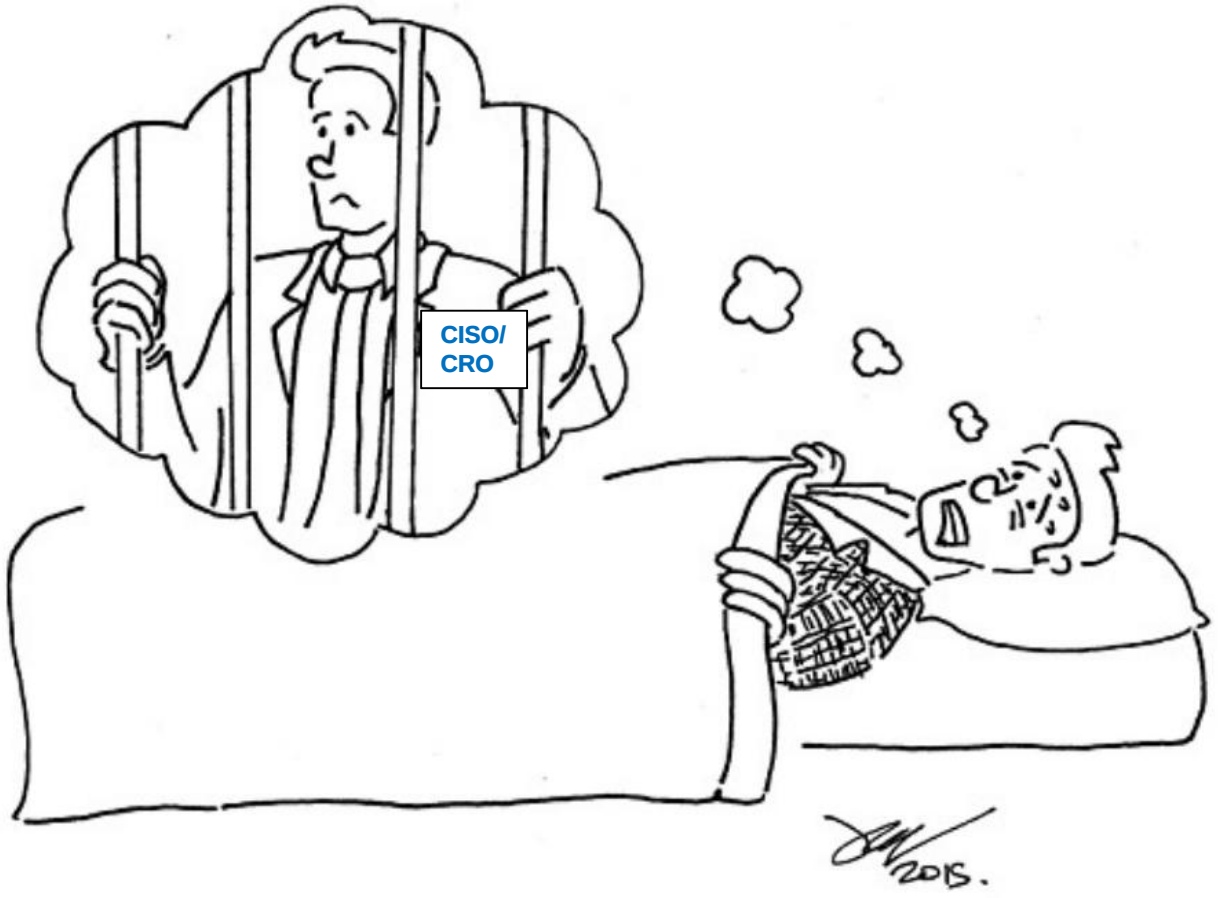
The Central Bank of Ireland (the 'Central Bank') recently undertook a thematic review to assess the management of cyber security and related operational risks across Investment Firms, Fund Service Providers and Stockbrokers. The objective of the review was to examine firms' control environment (including policies and procedures) designed to detect and prevent cyber security breaches as well as board oversight of cyber-security.

Cyber security is steadily emerging as an individually recognised risk in all firms. This is primarily due to the increasing reliance by firms in all sectors on information technology ('I.T.'), the evolving sophistication of cyber-crimes and the growing frequency in the type and number of cyber related breaches, attempts, attacks and intrusions. Valuable assets including confidential data, cash and intellectual property should therefore be protected by appropriate security, processes and policies.

Firms should be aware that cyber security risk is a real and live threat and a successful attack could have a significant negative impact on daily operations. Firms need to recognise that a successful cyber-attack can also have far reaching financial and reputational implications; therefore appropriate levels of security are required to be in place.

It is the board's responsibility to ensure that a firm is properly governed and has the necessary processes and systems to protect the firm and all of its assets. The review found that in a number of firms I.T. security, including cyber security, is deemed to be the sole responsibility of the I.T. department with limited involvement, if any, from other business areas or from the board itself.

Will this keep the CRO/CISO awake at night?



Thank you

Contact Peter Oakes to discuss non-executive director & consulting services for regulated financial entitles, fintech & other innovative companies

https://ie.linkedin.com/in/peteroakes

peter@peteroakes.com

+353 87 2731434 / +44 75 635 26834