BAE SYSTEMS

# Know your enemy

## How banks can identify and beat the evolving threat of financial crime

# Executive summary

**Szu Ho,** Financial Services Cyber Security Lead, BAE Systems

Banks need to know their customers (KYC) – but they need to know their enemies (KYE), too. Banking has changed dramatically in the past two decades, and adversaries have evolved to match. From mobile apps and contactless to wearables, technology has transformed how and where we bank – and how and where criminals act.

The industry must move fast and think smart to stay ahead of those who seek to subvert it. Financial crime is increasingly sophisticated, global and varied. And it is very often cyber enabled.

Pinning down typical perpetrators is harder than ever.

We are seeing increasing collaboration between groups of criminals across the wider landscape of serious and organised crime – something[1] we have profiled[2] before. Attackers' ingenuity[3] in identifying and exploiting new banking vulnerabilities is also growing. We are encountering both new types of fraud – including video and mobile takeover – and a resurgence in older methods, such as counterfeit cheques[4].


It has never been more important to build insight into the range of adversaries banks face – and the best ways of thwarting them.

[1] https://www.baesystems.com/en/cybersecurity/feature/the-unusual-suspects

[2] https://www.baesystems.com/en/cybersecurity/feature/the-invisible-network

[3] https://www.bankinfosecurity.com/payment-fraud-criminals-enroll-stolen-cards-on-apple-pay-a-12779

[4] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

## The financial crime line-up

With so many possible methods of committing financial crime, the list of adversaries is very long, says Nick Ryder, Professor in Financial Crime at the University of the West of England. "The scary thing is that it can be anybody. It's reasonable to suggest that anybody with a mobile phone or access to the internet can be a terror financier," he says.

While financial organisations, regulators and law enforcement agencies cannot expect to create a definitive list of criminals, they can identify characteristics and patterns of behaviour common to different types of fraudster. These insights may not offer the whole picture, but they provide solid ground on which to build strong but agile defences.

One threat to which banks and law enforcers must pay careful attention is white-collar crime and insider fraud, says Ryder. "One of the problems here is that companies can be reluctant to bring charges against the individual because of the bad publicity that will arise. So in some cases they will just dismiss them." Of course for those investigating fraud in the short and long term this is not helpful.

### Hazard warning
## The criminal insider

Outwardly holding down a position of trust, the insider is secretly passing crucial business and customer information to a criminal network. This individual might be working willingly or under coercion. The insider may not be the direct attacker, but rather be tasked with weakening defences or turning a blind eye to strikes. Well-intended security training may inadvertently benefit such activity.

Creative criminals will find new ways to disguise their activity. Ryder suggests banks look closely at seemingly legitimate operations – "...things like people testing their online security. This is a growth area for criminals." Putting a stop to security testing to halt a single attack vector does more harm than good. "From a government and national security perspective it's crucial to have security up to date," he says.

Banks also have a duty to communicate about fraudster behaviour with their customers. "Banks really need to make their consumers more aware of things like sophisticated email scams claiming to be from the 'Inland Revenue', for example. If people are new to the internet then they're going to be susceptible."


## The changing landscape

The criminal profile is constantly evolving, says Ryder: "Once we become cashless, fraudsters will move away from cold-calling to more online scams. Banks will need to be more aware of how they report allegations of fraud to the police and the National Crime Agency via a Suspicious Activity Report (SAR)."

Ensuring these reports are of real value will allow banks to build enemy awareness. This will require a change, says Ryder. "Too many SARs of low-quality intelligence are submitted and it is important that banks are more confident in their financial crime reporting systems and provide more detailed SARs."

Again this comes down to a better understanding of compliance and security. In fact, the Financial Conduct Authority (FCA) recently fined Bank of Scotland £45.5 million[5] for failing to disclose information about its suspicions that fraud may have occurred at the Impaired Assets team of Halifax Bank of Scotland. The FCA said that this negligence delayed scrutiny of the fraud by regulators, the start of criminal proceedings and the compensation process.

One of the key difficulties in knowing the enemy is that criminals are always going to be 10 steps ahead of financial institutions, says Ryder: "Laws are always going to be reactionary, as are policies, so it's like fighting a fire with a small garden hose." Prevention and early warning systems are key.

"It comes down to knowing your customer and their behaviour really well, as well as recent trends. Which countries are deemed to be at risk and which countries have weak levels of compliance, for instance? That's where the banks will be involved in de-risking," he adds.

[5] www.fca.org.uk/news/press-releases/fca-fines-bank-scotland-failing-report-suspicions-fraud

## Hazard warning
## The money launderer

The money launderer is usually working as part of a group. Red-flag behaviours include reluctance to provide information; incomplete or inconsistent information; unusual or unpredictable transactions.

Their networks could be vast and far-reaching, but they'll also be doing their best to cover their tracks. The trail might seem to disappear into thin air.

# What motivates financial crime?

In order to start identifying attackers more effectively, banks must build insight into the motivations of financial fraudsters, says Ryder. "It's mostly greed, of course, but there are other reasons, such as disrupting infrastructure, terrorism and [causing] reputational damage."

# Links with organised crime

Financial crime has evolved from password theft and hijacking online banking sessions. Fraudsters are using more diverse methods. We can use information about the resulting attacks on banks to identify emerging types of perpetrator.

Recently, we've seen core banking and interbanking systems being targeted – for instance in the 2018 Cosmos Bank ATM[6] attacks, where criminals compromised ATM payment authorisation and used fake debit cards to withdraw over $13 million in more than 14,000 transactions across 29 countries.

Also in 2018, an attack on SPEI[7], Mexico's domestic interbank payment network, cost multiple financial institutions more than $15 million.

So how can we use these experiences, drawing important lessons from history to build a clearer picture of our attackers?

---

[6] www.computing.co.uk/ctg/news/3061187/atm-hackers-steal-usd135m-in-28-countries-from-indias-cosmos-bank-just-days-after-fbi-warning

[7] https://uk.reuters.com/article/us-mexico-cyber/unauthorized-transfers-siphon-funds-from-mexican-banks-central-bank-idUKKBN1IC2PZ

# Hazard warning
# The cyber criminal

Operating as part of an organised gang or as a lone agent, the modern-day hacker could feed the critical information gathered to wider networks, facilitating attacks. The cyber criminal profile varies widely because personal motivation is key. This individual might want to bring down a national banking system, frustrate society or steal millions.

The answer lies in The Cyber Threat Landscape: Confronting Challenges to the Financial System[8], a 2019 paper by BAE Systems Applied Intelligence threat intelligence experts Adrian Nish and Saher Naumaan for the Carnegie Endowment for International Peace, which did just this, looking at historical attacks and highlighting worrying trends.

The report showed that attackers are building increasingly advanced capabilities to target core banking systems, particularly in payment messaging and transaction authorisation. They are also becoming more aggressive in their disruption of their victims' ability to respond to attacks.

Once their tools are built, attackers will use them for as long as they remain effective. As security is tightened around certain technologies, they immediately look for other ways to strike.

Criminal collaboration across borders and the proliferation of dark web online marketplaces offer plentiful tools and services that frustrate efforts to pinpoint the enemy.

This, says Szu Ho, Financial Cyber Security Lead at BAE Systems, allows previously disparate or under-skilled criminal elements to combine to potentially devastating effect, bringing together serious and organised crime. "This is driven by increasing specialisation and division of labour. Examples of this collaboration include the attacks on July 20, 2016, where cyber attackers attempted to steal $150 million from a bank in South Asia and then minutes later attacked a bank in West Africa for the same amount. Clearly attackers can coordinate and collaborate in complex attacks across different continents."

The paper from the Carnegie Endowment for International Peace predicts that though cyber criminals are likely to begin targeting markets and market participants, perhaps attacking foreign-exchange markets and securities, they are also unlikely to drop the tried and tested approaches that have served them well in the past. So while there are new types of criminal emerging, more traditional fraudsters still abound. What is more, movement between types is common.

[8] https://carnegieendowment.org/2019/03/25/cyber-threat-landscape-confronting-challenges-to-financial-system-pub-78506

## Hazard warning
## The organised criminal

This attacker could be at the head of various operations, with money laundering and fraud linked to serious crimes such as drug- and people - trafficking. Warning signs include heavy credit card use or large deposits in unusual places. The organised criminal will have fingers in various illegal pies, with an extensive network of hackers, underworld criminals and, possibly, insider fraudsters.

"We can see criminals are moving up the financial value chain from attacking lots of targets with smaller rewards to smaller numbers of targets with higher rewards," says Ho.

"Attacks are becoming more focused and efficient and they are yielding greater returns. We see that in more sophisticated attacks. The criminals get access to the target bank's networks and then loiter, maybe for up to 18 months, quietly observing and recording how the bank works, identifying potential weaknesses and laying the groundwork for their attacks by deploying malware and gaining access to critical systems. The actual attacks to steal the money can be over in hours."

# Cyber security lessons for the fight against financial crime

There are clear lessons that anti-money laundering and fraud prevention specialists can learn from their cyber crime-fighting colleagues to build a more nuanced overview of the threat. The FCA is calling for more collaboration between these camps.

Cyber crime is a relatively new area and is more concerned with the threat than is AML and fraud prevention work, which has traditionally been more compliance oriented. This focus on threats is important as it is directly aimed at identifying types of cyber criminals and what they are doing. "Cyber experts are more used to sharing information and have developed a common language to talk about threats and common protocols which fincrime does not yet have."

But there are distinctions to be considered. "Arguably, there is less of an issue with cyber threat intelligence sharing as this is to do with technical information and modus operandi

of attackers so there's no personal information. The attackers are not going to complain to the authorities about sharing information" explains Ho.

In contrast, information sharing for defenders is more fraught. "It has been traditionally more difficult to share fincrime information due to bank client confidentiality issues and the potential legal risks, as well as the difficulties of dealing with different regulatory and country regimes."

## In with the new, but not out with the old

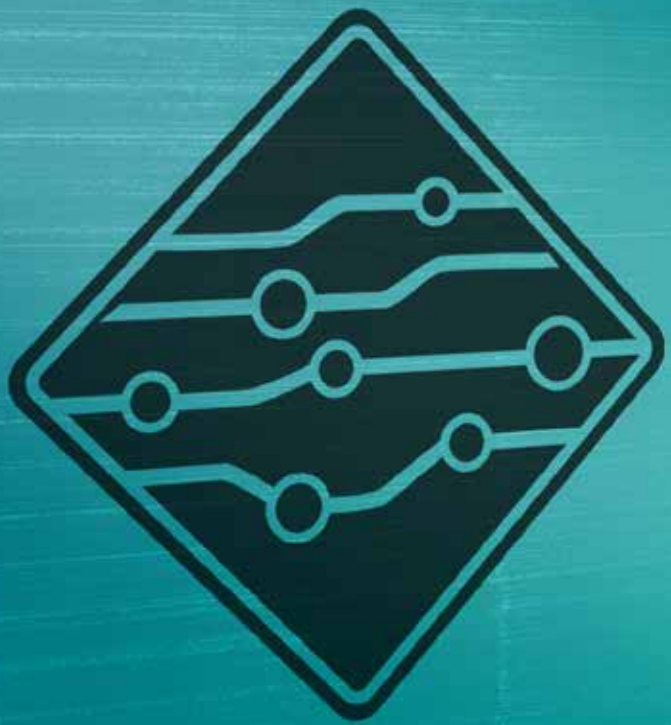
By looking at an overview it is possible to identify new categories of fraudster. In recent fraud cases, for instance, criminals have effectively hijacked mobile phones to intercept alerts and texts.

Richard Graham, Head of Business Solutions (Americas) at BAE Systems Applied Intelligence, believes this type of technical takeover crime is significant. "Phones were never intended to be verification devices, so they are now the weakest security link in a lot of ways," he explains. "If you change your password, your bank will send a verification message. If you log into your online banking account from a new computer, you get a text sent to your phone."

Attackers simply use compromised identities to log into existing mobile phone accounts and convince the phone companies to port the number to a new device.

## Hazard warning
## The early adopter

Happy to make use of any new tech available to extract money from the public, the early adopter is always one step ahead of the game. Methods include anything from mobile takeovers and video scams to AI-enabled fraud and biometric hijack. For every new technology, this tech-savvy criminal has worked out how to exploit it.



In other cases, an insider in the phone store or within the call centre facilitates takeover. The result is the same, says Graham. "Your phone no longer works and someone else has been able to send fraudulent payments out of the bank through your account with their device getting all of the authentication messages."

Identifying this individual is rendered harder because of the criminally valuable anonymity afforded by mobile technology. Graham says: "You can walk down the street and use your neighbour's Wi-Fi or go to a coffee chain."

This type of criminal is unlikely to limit their activity to mobile phones. Video has clear persuasive potential as a new social engineering vehicle.

The rapid development of biometrics in banking is another area of concern. Could financial criminals become more violent – physically forcing their victims to comply with checks? While Graham does not expect this to be a significant phenomenon, complacency about the potential of biometrics for evolving criminals is not an option.

"I think it's more likely that high-powered cameras will be used to take photographs. If you can get a person's fingers at a great enough resolution, you could 'print' their fingertips, rendering fingerprint biometrics useless for certain people in the long run."

Ultimately, he says, new opportunities for crime will present themselves, giving rise to new groups of perpetrators. "Where there's a will, there's a way," he concludes.

However, as new methods attract the attention of the equally technically expert cyber security professionals, are some criminals going retro? Digital vigilance is heralding a resurgence of old-school tactics, such as cheque counterfeiting.

## Hazard warning
## The retro fraudster

This old-school criminal has worked out that while technology has developed apace, with consumers increasingly good at recognising commonly known scams, they might reduce vigilance in other areas. The retro fraudster runs Ponzi schemes, bounces cheques and creates fake jobs. The sums involved are often small enough to pass undetected. Digital technology can update and facilitate some of the oldest tricks in the book.

Brian Ferro, Head of Global AML and BSA Compliance Product Management, BAE Systems, views this type of fraud as a growing trend, particularly in the US where cheques are in regular use. "We're seeing a combination of new channels and old-school tactics emerging," he says.

"With the advent of higher quality personal printers, it's much easier to make your own cheques or to copy other customer or cashier cheques," he explains. Other low-tech scams are also growing. One example is fraudulent job adverts, which then invite 'successful' applicants to pay money up-front for equipment.


Executive scams have also seen a resurgence, such as old fashioned invoice hacks, where the fraudulent issuer persuades an accounts department to send remittance to the wrong place. When payments are for modest sums, says Ferro, the illegal movement of money often passes under the radar.

"These are old tricks but using digital channels," says Ferro. While the younger generation is more aware of digital security problems, it is less knowledgeable and wary of these seemingly old-fashioned crimes. "They might be very savvy when it comes to email or online crime, but wouldn't even consider someone going to the trouble of creating a counterfeit cheque," he says.

The age-old Ponzi scheme (where investors are lured in by promised high rates of return from sales of a non existent product or service), at its peak in the 1920s, has been brought up to date.

Ferro says: "Now they're just doing a better job with marketing and falsifying. They are leveraging new tech to manipulate numbers and connections – counterfeiting the investment health instead of the money."

Key to combating this, once again, is really knowing the customer. "It's about being very vigilant about how you monitor, say, excessive payments from the over-55 segment," says Ferro.

"Many banks are realising their place in society and doing more to help their customers. The Bank of Montreal [which has recently launched its own financial crimes unit] is doing strong work in reaching out to its customers in this area."

As tech gets more sophisticated, the simpler things tend to be neglected, says Ferro, but vigilance is vital. "It's about the obvious but not readily apparent ways we end up getting duped."


## Conclusion

The criminal landscape may be busy, with new threats evolving all the time, but the financial sector is getting better at frustrating them. Increased collaboration – such as the Customer Security Programme operated by the global financial messaging provider SWIFT – is helping to ensure banks and financial institutions start sharing best practice, hard lessons and valuable information on the particular types of attacker.

Comprehensive profiles of likely fraudsters would seem the most valuable solution. And various organisations, such as the inter-governmental Financial Action Task Force, are helpful here, issuing members with regular updates on known perpetrators and the financing of terror.

Criminals have learnt to vary their methods and disguises and to collaborate. We must do the same by breaking down the traditional information silos between cyber security and fincrime teams within institutions.

Only then can we properly identify and beat the evolving threat of financial crime.

# What next?

A well-structured organisation is the foundation of a robust defence against money launderers and fraudsters. Start by identifying the skills, capability and technology you already possess before considering solutions.

**Break down walls**

All too often internal expertise that could be put to use to identify threats is not applied to the problem. This is all the more troublesome if resources are tight, demand for the skills of teams of individuals is in high demand, or siloed in organisational fiefdoms. You can find out more about how to do this at baesystems.com/problem-shared

**Check your cyber preparedness**

While high-volume attacks against personal banking customers may require relatively little effort, attackers are also becoming more effective at targeting banks directly. Working with industry bodies such as SWIFT on attestation programmes and educating customers and staff will help identify potential weaknesses while actively building defences.

**Socialise and network**

Preparing defences in isolation often results in oversight. Sharing information, intelligence and challenges with peers, regulators and law enforcement in a structured environment is usually helpful and productive for all. To do this, collaborative frameworks and encouragement from government are vital, so proactively advocating for intelligence sharing and closer co-operation in a setting that maintains confidentiality can help shift mindsets.

For more information go to: **www.baesystems.com/bankinginsights**

## Contact us

E: learn@baesystems.com
W: baesystems.com/bankinginsights

**Victim of a cyber attack? Contact our emergency response team on:**

US: 1 (800) 417-2155
UK: 0808 168 6647
Australia: 1800 825 411
International: +44 1483 817491
E: cyberresponse@baesystems.com