Preventing institutional payments fraud

Basic defences, counter measures and best practices

SWIFT ebook
January 2019

What will we cover?

Fighting fraud

Arm yourself with solutions for preventing institutional payments fraud

The fraud threat: Where do we stand today?

"Financial institutions and payment infrastructures are the new targets"

Source: 2017 Payment threats and fraud report, European Payments Council

More than ever, financial institutions and payment infrastructures are being targeted by cyber attackers, who are innovative and work with subtlety, sophistication and patience. Cyber attackers cover their tracks and exploit the fact that payments move faster than ever.

Threats are increasing with patterns of wire payment fraud on the rise, up from 14 per cent in 2014 to 48 percent in 2017 (source: 2018 AFP® Payments Fraud and Control Survey). The risk of institutional payments fraud continues to shake the industry. And in the wake of the Bangladesh Bank heist in 2016, we have seen similar attacks across a number of other banks worldwide.

Institutional payments are an attractive vehicle for criminals due to the speed and finality of settlement. Added to this, originators and volumes continue to grow, expanding the collective target.

Could you fall prey to institutional payment fraud?

The growing threat of cyber attacks has never been more pressing as criminals move from data theft to committing institutional payment fraud - and banks need to be able to verify the integrity of payments in real time.

When you understand the changing tactics fraudsters employ to perpetuate institutional payments fraud, prevention becomes easier. Ensuring that internal controls and strategies are in place will help protect your financial assets. So, if you haven't already considered solutions available to help defuse the threat, your electronic transfers could be at risk.

Modus operandi of a cyber attack

Cyber attackers don’t want you to understand what they’re doing. The less you know, the more opportunity they have to fraudulently extract funds from your organisation.

1

Cyber attackers compromise member’s environment

- Malware injected by email phishing, USB device, rogue URL or insider compromise
- Long reconnaissance period monitoring banks’ back office processes

2

Cyber attackers obtain valid operator credentials

- Keylogging / screenshot malware looking for valid account ID and password credentials

3

Cyber attackers submit fraudulent messages

- Attackers impersonate the operator / approver and submit fraudulent payment instructions
- May happen outside the normal bank working hours / over public holidays

4

Cyber attackers hide the evidence of their actions

- By deleting or manipulating records/ log used in reconciliation
- By wiping the master boot record

Authorities across the globe have taken regulatory and supervisory steps to facilitate both the mitigation of cyber risk by financial institutions, and ensure effective response to, and recovery from, cyber attacks.

Financial Stability Board (FSB) member jurisdictions have actively addressed cybersecurity, with all member jurisdictions releasing regulations or guidance that tackle cybersecurity for the financial sector.

All FSB member jurisdictions report drawing upon a small body of previously developed national or international guidance or standards when developing their own regulatory or supervisory schemes for the financial sector.

A third of reported regulatory schemes take a targeted approach to cybersecurity and/or information technology risk and the remaining third address operational risk generally.

Common elements covered in cybersecurity regulation include risk assessment, regulatory reporting, role of the board, third-party interconnections, system access controls, incident recovery, testing and training.

Jurisdictions remain active in further developing their regulation and guidance.

International bodies have also been active in addressing cybersecurity for the financial sector, with a number of similarities across international guidance issued by different sectoral standard-setting bodies and other international organisations.

Best practices

“There has been a 1,700% increase in cyber attacks reported to the FCA since 2014.”

Source: Financial Conduct Authority

Following these best practices can help mitigate your exposure to cyber threats.

Ensure good payment hygiene

While many banks rigorously check confirmations and statements, others are unaware these practices can mitigate the risk of fraudulent attacks on their back offices, and are further unaware of how to respond when they do happen.

Understand the threat

Knowing your adversary is vital to protecting yourself against it.

Limit your exposure

You should only do business with trusted counterparties – and only maintain relationships with those you trust.

Implement security controls

Engaging in regular security benchmarking and audit exercises enables you to detect gaps and lapses in your security controls.

Know your counterparties

Your understanding of potential counterparts’ cyber and compliance risks is key to your decision-making around whether and how to do business with them.

The quicker something is identified as fraud the more likely it will be stopped.

Failure to secure your systems and networks leaves you exposed to attack. No system is totally bulletproof, but there are ways to protect your organisation from the complex methods being used against you – these include being prepared for attacks succeeding.

Strength comes from multiple layers of defence, which are essential to combat the threats our community is up against. This means safeguarding both logical and physical security, as well as ensuring additional defences around critical systems, and putting detection measures in place around and within them to identify potential intruders.

Take action to safeguard your local environment and reinforce the security of the global financial community.

Secure your environment

Know and limit access

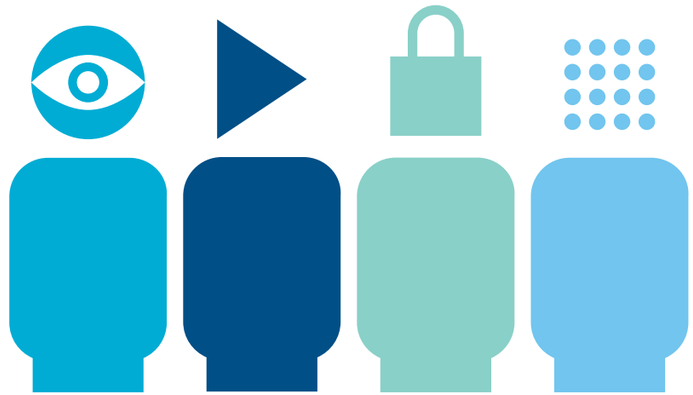
Detect and respond

“Cyber attacks are now the third biggest risk in terms of likelihood, trailing only natural disasters and extreme weather events.”

Source: Global Risks Report from the World Economic Forum

The rise in the threat level requires a concerted response. While you are responsible for the security in your own organisation, a community-based approach is the best way to solve the security issues facing the industry.

And that is why the SWIFT Customer Security Programme (CSP) has been developed and will continue to evolve in close collaboration with our community. The CSP addresses three key aspects of your business and your relationships, enabling you to take action with the support of SWIFT’s programme.



A common threat.
A shared commitment.

This is a journey that involves SWIFT and its community of customers, regulators, overseers and third parties to collectively work together to fight against cyber attacks.

Our three-part framework

You
Secure and protect

You first need to secure and protect your local environment – this is the most important action you can take. Securing your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber fraud.

To support the industry, we have published a core set of mandatory security controls and an associated assurance framework for its users. The security controls build upon our existing security guidance, taking into account the latest intelligence on known cyber threats and incidents.

Your counterparts
Prevent and detect

Companies do not operate in a vacuum and all SWIFT users are part of a broader ecosystem. Even with strong security measures in place, attackers are very sophisticated and you need to assume that you or your counterparts may be the target of cyber attacks. That is why it is also vital to manage security risk in your interactions with counterparties, and consider a tool to protect your payment flows.

Your community
Share and prepare

The financial industry is global, and so are the cyber challenges it faces. What happens to one institution in one location can easily be replicated elsewhere.

If you have been targeted or breached, it is vital to share all relevant information and let us know there is a problem as soon as possible. SWIFT will then share anonymised information or Indicators of Compromise (IOCs) across the community to help limit further impacts. We will inform you of relevant cyber intelligence, and continue to expand our information sharing platforms to do so.

While many banks rigorously check confirmations and statements, others are unaware these practices can mitigate the risk of fraudulent attacks on their back offices, and are further unaware of how to respond when they do happen.

Protect your core payment systems

Having relevant and timely intelligence helps protect you from cyber threats. **SWIFT Information Sharing and Analysis Centre** (SWIFT ISAC) allows you to share intelligence on cyber attackers' latest strategies and activities with your community and use this information to adapt your defences.

You can then use **Daily Validation Reports** to profile your normal payment flows and validate your payment logos against SWIFT data to prevent cyber attackers covering their tracks.

Once you have the insights, you can take decisive action. **SWIFT Payment Controls** simply and effectively flags and intercepts suspicious payments to protect you and your counterparts. The overall goal is to reduce fraud and reputational risk and to build trust between institutions across the SWIFT community.

Established relationships can change over time and may not be aligned with business patterns today. With the **Relationship Management Application (RMA)**, you can control who sends messages, and also restrict the types of messages with RMA+.

Build trust
SWIFT ISAC

- Understand latest attack strategies and activities
- Harden your defences in response
- Build trust for you and your community
- Understand how to avoid being an easy target for cyber attackers

Reduce reputational risk
Daily Validation Reports

- A complete and accurate view of your transactions over SWIFT
- Validate your daily payment flows
- Identify suspicious anomalies
- Delivered directly to your compliance or operations team

Reduce fraud risk
Payment Controls

- Real-time transaction monitoring
- In-network security
- Sophisticated, flexible rules based on your real data
- Fast incident response

Building a more secure future - together

The fraud threat is adaptive, so we are devising innovative ways of countering the threat and actively investigating cases and potential threats.

This involves informing you of threat indicators through the SWIFT ISAC, and providing you with the solutions you need – including Daily Validation Reports and Payment Controls - to help protect your local environments and ensure that your ongoing security updates assist in countering the very latest tactics.

Find out more

Fraud control
Customer Security Programme
Contact us

About SWIFT

SWIFT is a global member owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community's access and integration, business intelligence, reference data and financial crime compliance needs. SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's international office network ensures an active presence in all the major global financial centres.

For more information about SWIFT, visit **www.swift.com**.

We can do more together

At SWIFT, we help to protect, shape and enhance the financial future of our members, their customers and the communities they support.

Our Global Payments Innovation (gpi) is transforming the effectiveness of cross-border payments by leveraging our deep experience and the right technology. This ensures transactions are predictable, as well as fast, transparent, trackable and secure, end-to-end.

Our Customer Security Programme (CSP) is reinforcing the security of the global financial community by harnessing the strength of the SWIFT network and focusing on the security of local environments. This ensures we all work together to protect and advance the security of the global financial community.

Our financial crime compliance solutions are easing the ever-growing compliance burden for our community and helping our members play their part in preventing criminal activity.

www.swift.com/complianceservices

57393 - January 2019