Information paper

From security baseline to best practice

Securing India's critical channel infrastructure

Contents

Executive Summary

In recent years the financial community in the Indian subcontinent has fallen victim to substantial wire frauds. External and internal malicious actors have successfully compromised the operating environment of the banks, stealing or misusing SWIFT operator credentials, executing fraudulent transactions and obfuscating the attacks. In response, the RBI has introduced strict operating controls, imposing fines in cases of non-compliance, and continues to audit and monitor SWIFT channel operations. The threat of cyber attacks on banks and their critical channel infrastructure, including SWIFT, is persistent and increasingly sophisticated.

This paper provides a summary of recent SWIFT threat intelligence, explaining how malicious attackers are evolving and the patterns of wire fraud financial institutions can use to improve their monitoring of anomalous transactions. We also describe key developments in the Customer Security Programme (CSP) which is available for the SWIFT community in the Indian subcontinent to leverage in response to these threats. These include:

a) the Customer Security Control Framework (CSCF) v2019, which will uplift the controls required in the operating environment of SWIFT users;

b) the Payments Control Service (PCS), a zero-footprint, in-network screening utility which offers a last line of defence in the event your operating environment is compromised;

c) quality and timely data for reconciliation to enable timely detection and response to active attacks; and

d) SWIFT messaging infrastructure features to strengthen multi-factor authentication and integration with enterprise authentication systems.

Along with an aggressive regulatory agenda, pressing demands from domestic consumers, and continuing competition from incumbents and new home-grown and foreign entrants have set a fast-paced roadmap for digitisation in financial services. While short and medium term challenges remain, digitisation will be a key enabler for India to achieve its forecasted 7.6% GDP growth in 2019-20 FY, putting it ahead of its BRICS counterparts.

Cybersecurity poses a significant threat to this roadmap. IT and operations executives at financial institutions should instil a culture and discipline of security while mindfully enabling the enterprise with new digital capabilities to combat looming threats.

SWIFT is committed to supporting our community in responding to persistent threats targeting our community in the Indian subcontinent. Contact us at csp.apac@swift.com to find out more.

India's march to a digital economy

This section is based on BCG analysis of RBI data, FIBAC Productivity Survey 2016, 2018 Cybersecurity Market Report by Cybersecurity Ventures, 2018-19 EY GISS India reports, 2018 Gartner research and other public sources. See the References section for a list of sources.

An increasing rate of digitisation, leading to a more complex attack surface

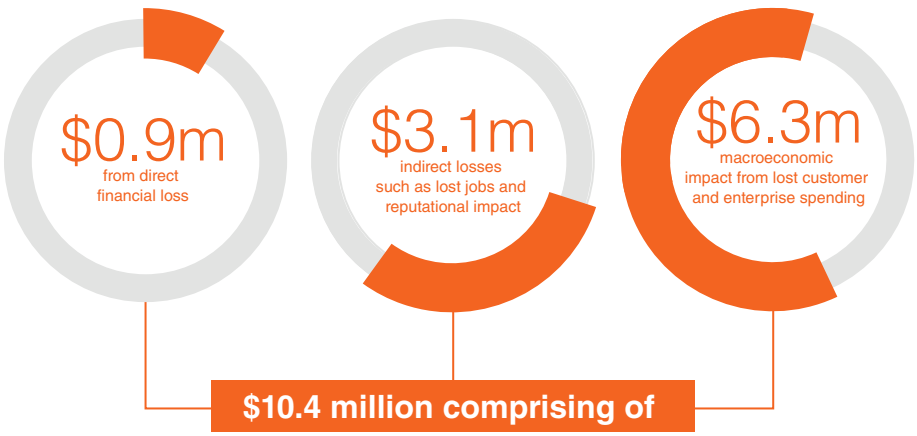
With an annual GDP growth of 7.6% forecast for 2019-20 FY India is well on track to break away from the BRICS pack as its leading economy. An aggressive roadmap of digitisation driven by customer demand, competition and regulatory pressures led particularly by the financial services sector is a key enabler of this growth.

The increasing rate of digitisation of Indian financial institutions over the last two years is reflected in the adoption of digital instruments and channels. RBI data shows the Unified Payments Interface platform has reached 3 billion transactions in two years; point-of-sale card transactions have doubled to 22 billion transactions in three years; mobile transactions have tripled to 15 billion transactions in one year, all driven largely by continuing penetration of smartphones and the availability of cheaper data.

While digital channel transactions have grown by 48%, physical branch and ATM transactions have declined by 11% and 5% respectively. In a risk-averse culture where cash under the mattress is the norm, this is a marked shift in customer preference from physical to digital channels.

Sophisticated cyber threats persist

Over the last few years cyber threats have created a significant challenge for the Indian financial services sector. Recent high-profile incidents, subsequent regulatory requirements and fines have significantly impacted firms and their mission to service their clients. According to Cybersecurity Ventures the average cost of a cyber attack on Indian firms, across all types of incidents, is estimated at $10.4 million[1].



Average cost of cyber attacks in 2018, across all types of incidents (Source: 2018 Cybersecurity Market Report, cybersecurityventurres.com)

EY analysis shows cyber incidents also impact firms' market capitalisation, with share prices falling by an average of 5% after a cyber incident has been disclosed. Over 30% of customers affected by a breach ended their relationship with that organisation[2].

The frequency and persistence of the threat is continuing to increase. Reserve Bank of India (RBI) data estimates Indian banks fell victim to 130,000 reported cases of cyber fraud involving an estimated Rs 700 crore or $101 million from 2008 to 2017.

More resources and investments are being devoted to strengthening cybersecurity

In India, cybersecurity expenditure is expected to exceed $1 trillion from 2017 to 2021[4]. In 2018, the average banking and financial services firm allocated 7.8% of its total annual IT spend on security investment and operations[5]. The noticeable rise in cybercrime has driven IT security budgets upwards so fast that researchers and analyst firms are having difficulty forecasting future expenditures.

While the funding tap is opening wider, there is a large gap in talent. In 2015, Frost & Sullivan forecasted a global shortage of 1.5 million workers by 2020. In light of recent events, this has been revised upward to 1.8 million worker shortage by 2022.

India, too, is likely to see significant growth in the cybersecurity market over the next decade. According to the Data Security Council of India (DSCI), a staggering nine-fold increase in the cybersecurity market is expected by 2025, taking its current $4 billion to $35 billion. This will be fuelled by an ecosystem of indigenous security products, services and start-up companies.

Shareholders and Boards of Indian firms have taken note, recognising that mitigating cyber attacks is an aspect of their fiduciary responsibilities, 62% are taking active steps to strengthen their understanding of cybersecurity, technology and the threats that these events pose to the business.

Yet firms feel unsafe

It seems that the glut of news coverage, the impact to business, increased spending and tightening focus are keeping business leaders awake at night. A survey of IT and security executives by EY GISS India found that only 6% of financial services firms say their information security function currently meets their organisation's needs. 31% identify skills shortages as a potential obstacle[2].

While respondents in financial services scored themselves higher than those in other sectors, financial services executives are most concerned about the immaturity of their information security architecture and processes. As an example,18% cited information security metrics and reporting, and 17% cited asset management, as non-existent or immature. Only 16% of financial services sector respondents said their reporting of information security meets their needs[2].

As India marches towards an inclusive digital economy, an engine of future growth, the risk of cyber attacks poses a significant threat. Cyber threats will not stop, however they can be contained and mindfully managed. This will require the private sector to prioritise investment and talent, bolstered by sound state and government policies designed to facilitate cyber literacy and education, intelligence sharing and joint incident planning and exercises.

Number of reported incidents according to CERT India (Source: CERT India annual reports)[3]

Cyber threats targeting SWIFT users are evolving

This section draws from the **SWIFT ISAC Report - Three years on from Bangladesh: Tackling the adversaries** *(April 2019).*

In recent years the financial community in the Indian subcontinent has fallen victim to substantial wire frauds. External and internal malicious actors have successfully compromised the operating environment of the banks, stealing or misusing SWIFT operator credentials, executing fraudulent transactions and obfuscating the attacks. In response, the RBI has introduced strict operating controls, imposing fines in cases of non-compliance, and continues to audit and monitor SWIFT channel operations. The threat of cyber attacks on banks and their critical channel infrastructure, including SWIFT, is persistent and increasingly sophisticated.

As part of the CSP, SWIFT established an Information Security and Analysis Centre (ISAC) and periodically publishes modus operandi, tactics, techniques and procedures employed by malicious actors to target SWIFT users.

The Customer Security Intelligence (CSI) team works with targeted SWIFT users to conduct investigations and derive anonymised intelligence for publishing as bulletins in the SWIFT ISAC. In the three years the CSP has been in effect, SWIFT has published multiple bulletins, providing valuable insights into how cyber prevention and detection measures should evolve.

In 2018, SWIFT set out to increase its collaboration with law enforcement agencies and industry experts including anti-virus vendors and incident response teams. These efforts have paid off with more rapid identification of financial institutions targeted by cyber criminals – in most cases before fraudulent transactions were even sent.

Most of these attacks were identified and intercepted in the preparation phase. However, in a subset of the attempted attacks, fraudulent cross-border payment instructions were issued by the attackers. Even here, however, many of these fraudulent instructions were later stopped thanks to the intervention of banks along the payment chain.

In April 2019 SWIFT published an ISAC report describing the trends we have observed through 2018 and 2019. These have showcased how both business and security information can identify red flags and become key in detecting and responding to attempted attacks. This paper highlights the key observations of the report and we recommend SWIFT users read the full report available at **www.swift.com** titled "Three years on from Bangladesh, Tackling the adversaries".

Targets

In most cases, the target banks identified were in countries with a high or very high risk rating on the Basel AML Country Corruption List1. Over the last fifteen months, the majority of the attacks targeted financial institutions in Africa, Central Asia, South East Asia and Latin America.

In all cases the target institutions were smaller banks in terms of the number of cross-border transactions processed per day.

In the vast majority of cases investigated, fraudulent transactions were inserted using the Graphical User Interface (GUI) of the channel messaging interface. This means that the instructions would not have been present in payment back office applications. Strong reconciliation processes and quality reconciliation data is mitigating the risk of this attack technique. Financial institutions should establish automated reconciliation using data provided by the messaging interface along with copies of transactions provided by the SWIFT Transaction Copy Service (TCS) and request counterparties to send confirmation and statement messages of nostro accounts for the purpose of reconciliation.

Amounts

SWIFT's efforts to raise awareness, deliver new tools and services, and provide actionable cyber intelligence coupled with the investments and operations discipline of SWIFT users have thwarted many potential attackers over the last three years. Fraud monitoring and screening utilities deployed in response to these incidents have also played an important role. Rules defined in these utilities will need to be periodically adapted if they are to continue to be effective.

Sending fraudulent high value payment instructions can attract large rewards, but the higher the value of the instruction, the greater the risk of triggering fraud detection systems. Since the cyber incident in Bangladesh, the amounts sent in individual fraudulent transactions have been reduced, making them harder to detect. Until early 2018, we typically saw per transaction amounts of 10 or tens of millions USD. Since then, attackers have significantly reduced average per transaction amounts to between 0.25 MUSD and 2 MUSD with the aim of avoiding detection.

In each attack we investigated, most of the transactions issued were handled by one or two Receiver banks and were intended for the same Beneficiary country. During the most recent investigations, the number of fraudulent transactions issued averaged around 10 per incident, all sent within a two-hour period.

Reconnaissance

Tempted by the prospect of potentially lucrative pay-outs, attackers are persistent. They will often penetrate a target and wait for weeks, or even months, before launching an attack, using this time to learn patterns and behaviours and plot their fraud. Whilst they operate "silently" during this reconnaissance, it is a critical period for detection.

The initial response to a detected intruder is vitally important, even if there is no evidence of actual or attempted theft.

Timing

Timing is critical in determining the success of a cyber attack. The following graphics illustrate the role this by showing the local times at which fraudulent transactions were sent.

Two main patterns can be identified:

1. attackers try to send messages outside business hours or during public holidays in order to avoid detection by the target institution; or
2. attackers try to send messages during business hours to blend in with the legitimate traffic of the target institution to avoid detection by the counterparty and Beneficiary institution.

Fraudulent messages that go undetected for a longer period of time have a higher chance of reaching Beneficiary accounts and, as such, of being cashed out. Responding in a timely manner to cybersecurity incidents and having structured and tested reconciliation and cancellation processes in place can help reduce the financial impact of a cybersecurity incident.

In more recent incidents, however, the attackers have started to issue fraudulent payments during working hours on business days. Furthermore, the cash-outs have taken place within a matter of hours.

The two distinct ways of working can be seen here:

1. sending messages outside business hours or during public holidays in order to avoid detection by the Target institutions, and
2. sending messages during business hours to blend in with legitimate traffic to avoid detection by both Target and Beneficiary institutions.

Currencies

With the USD accounting for the majority of cross-border traffic, it is no surprise that this was the currency used in the majority of incidents investigated – approximately 70% of the fraudulent messages created since 2016.

Since then, however, we have also observed an increase in the use of European currencies – most notably EUR and GBP – while a small minority of incidents (approximately 5%) involved Asia Pacific currencies – mainly HKD, AUD and JPY. This demonstrates how important it is for Receiving Banks to pay attention to their customers' use of all these international nostro accounts, not only those in USD.

Beneficiaries

Attackers need Beneficiary or "mule" accounts in order to extract funds from the financial system. Those fighting fraud should be familiar with their profile.

Institutions must also ensure they are conducting strong due diligence on corporate and retail customers and their correspondent relationships. Poor Know Your Customer (KYC) creates opportunities for them to abuse the institution and use it to funnel fraudulent funds. This is damaging for both the victim institution and the institution operating the Beneficiary account.

The small subset of investigated cases where the adversaries managed to initiate fraudulent message instructions provides interesting data on the Beneficiary accounts. SWIFT was able to extract Beneficiary country information from the fraudulent messages sent in 2018 – information which revealed differences in pay-out techniques. What was most notable, however, was the concentration of the Beneficiary banks in the Asia Pacific: 83% of all fraudulent transactions had a Beneficiary account in this region. The remaining 17% was spread over other regions including, in order of magnitude, Europe, North America and the Middle East.

SWIFT's information sharing initiative has contributed to significant improvements in the SWIFT user community's collective cyber defences. SWIFT encourages all users to proactively contact and cooperate with SWIFT if they are targeted, or suspect they are being targeted, by malicious actors.

Contact us at **www.swift.com/support**.

SWIFT users must remain vigilant, going beyond baseline security to best practice

SWIFT Customer Security Programme (CSP)

Launched in 2016, the SWIFT CSP is based on three mutually reinforcing pillars. Customers first need to secure and protect their local operating environment (You), prevent and detect fraud in their commercial relationships (Your counterparts), and continuously share information and prepare against future cyber threats in collaboration with others (Your community).

Over the last three years the SWIFT user community has achieved a baseline level of cyber hygiene. To meet the challenges of an increasingly complex attack surface and an evolving threat landscape, SWIFT users in the Indian subcontinent must move beyond this baseline towards security best practices. The steps include:

- implementation of a payment screening utility such as the Payments Control Service as a last line of defence;
- integration of messaging and communications interfaces with enterprise authentication systems;
- using interface reporting data to strengthen reconciliation processes;
- compliance with uplifted controls defined in the SWIFT Customer Security Control Framework v2019 by end-2019; and
- integration of counterparty attestations to define and mitigate counterparty risk.

For more information on the SWIFT CSP, visit us at www.swift.com/csp.

A. Payments Control Service – your last line of defence

Security requires multiple layers of quality defence measures. While the CSCF brings much needed cyber hygiene to users' operating environments, there is also a need for effective and robust transaction screening.

As part of SWIFT's financial crime compliance portfolio SWIFT has introduced a zero-footprint, in-network payment screening utility. The Payments Control Service (PCS) enables customers to screen payment instructions safely, before transmission to counterparties, to detect any illicit or unusual message flows.

Using this tool, users can define their own monitoring policy, controlling their parameters to enable timely detection and prevention of out-of-policy or uncharacteristic, and therefore potentially high-risk, transfer requests.

The types of parameters defined in the PCS are specifically designed to address the wire fraud attacks we have observed impacting SWIFT users. Rulesets derived from these parameters can be defined for each sending Business Identifier Code (BIC) of the institution, offering granular control of your payments business.

By understanding the patterns of payments sent over time, such as the intelligence provided in Section 2, PCS enables users to implement more effective and robust controls. Monitoring rules can also be deployed in real-time to enforce policies and protect payment operations. This reduces the risk of fraud and gives operations teams tighter overall control. In the event that the institutions' operating environment is compromised, PCS offers a vital last line of defence.

B. Integrating with enterprise authentication systems

Multi-factor authentication is an effective way to mitigate the risk of malicious actors harvesting credentials. A second independent and robust factor prevents login and operations by privileged accounts even if username and passwords have been compromised by key loggers or screen-capture malware. Factors of authentication include something you know (passwords), something you have (tokens), or someone you are (biometrics).

SWIFT messaging and communications interfaces support the use of traditional usernames and passwords, time-based one-time-passwords (TOTP), and integration with RADIUS. Alliance Release 7.3 has further strengthened these. SWIFT interfaces now also support USB tokens and SAML 2.0 for integration with more sophisticated Identity Provider (IDP) systems.

TOTP is a common implementation of multi-factor authentication in the Indian subcontinent. This is often implemented using mobile devices such as smart phones and tablets. Unmanaged mobile devices in product environments carry inherent risks. SWIFT recommends users implement USB tokens or integration with IDP systems which may enable biometric authentication.

C. Using interface reporting data to strengthen reconciliation processes

Malicious actors rely on the delayed detection and reaction of SWIFT users to siphon funds out of the electronic banking ecosystem. Robust reconciliation processes improve the speed and efficacy of detection, and SWIFT interfaces provide the quality and timely transaction reporting data required. These include the following.

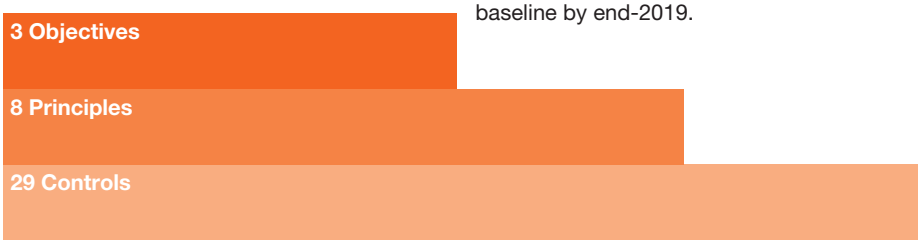
- Standard GUI-based reports show individual message history, aggregate message reports, evidence of manual interventions in message processing, and message types, across date ranges, value and currency. They can be manually exported to CSV, PDF, XLS or TXT formats.
- Operational command-line reports provide more detailed audit trail reports, exception statistics such as successful or failed messages, operator activity reports, and other reports that can flag nefarious activity.
- Customised reports are defined for your institution. They can show remitter and beneficiary details for fraud monitoring in formats required for consumption by back office and security monitoring systems.

D. Compliance to SWIFT Customer Security Controls Framework v2019

Malicious actors target the messaging and communications interfaces of SWIFT users to perpetrate wire fraud. By breaching the institution, stealing credentials, sending fraudulent transactions and obfuscating their attack, they aim to steal funds from counterparties' nostro accounts.

To establish a security baseline for SWIFT channel operations, SWIFT introduced the Customer Security Control Framework v1 (CSCF) in mid-2016. These mandatory and advisory controls are defined by SWIFT and industry experts and articulated around three overarching objectives: 'Secure your Environment', 'Know and Limit Access', and 'Detect and Respond'. The control definitions are in line with existing information security industry standards, and are product-agnostic. The mandatory and advisory controls, and associated policy, are published on the SWIFT Knowledge Centre on swift.com.

As malicious actors' techniques continue to evolve, there is a need to periodically uplift these controls. In mid-2018, an updated CSCF v2019 was published, upgrading three advisory controls to mandatory and introducing two new advisory controls. Financial institutions should implement necessary changes in their operating environments and comply with this new baseline by end-2019.



SWIFT Customer Security Controls Framework - Objectives and Principles	
Secure Your Environment	1 Restrict Internet access
	2 Segregate critical systems from general IT environment
	3 Reduce attack surface and vulnerabilities
	4 Physically secure the environment
Know and Limit Access	5 Prevent compromise of credentials
	6 Manage identities and segregate privileges
Detect and Respond	7 Detect anomalous activity to system or transaction records
	8 Plan for incident response and information sharing

E. Measure and mitigate your counterparty risk

Cybersecurity risks, including those introduced by counterparties, need to be managed together with operational, financial and regulatory risk. Many institutions are working to integrate cyber risk assessments into their existing counterparty risk processes.

For effective oversight and governance of this process the right people must have appropriate responsibilities and scope for decision-making. The processes must also be strong and repeatable. Institutions with an appropriate governance structure in place can define a cybersecurity risk management framework to assess risk and implement commensurate countermeasures. This includes the risk assessment of counterparties by:

- collecting the necessary data to support risk-driven decisions;
- processing this data and transforming it into a weighted, risk-based assessment, typically shown as a numeric score or a red-amber-green indicator;
- adopting suitable countermeasures to mitigate or 'treat' the risks.

Within this governance model and risk management framework, institutions should consider incorporating data on their counterparties' cyber-preparedness – and the SWIFT CSCF can provide an invaluable tool.

Attestations concerning the CSCF submitted by your counterparties are a source of this data. Once attestations have been published, SWIFT users can make them available to their counterparties using the SWIFT KYC-Self Attestation (KYC-SA) tool. The attestations are evidence of compliance per individual control and can be integrated into your risk-based decision frameworks. Mitigations may include additional monitoring and screening of particular counterparty transactions, a lower threshold or additional authorisations for account operations for the counterparty and, if necessary, removal of Relationship Management Application (RMA) authorisations.

For more information on these security best practices contact us at **csp.apac@swift.com**.

Are you prepared to respond?

Along with an aggressive regulatory agenda, pressing demands from domestic consumers, continuing competition from incumbents and new home-grown and foreign entrants have set a fast-paced roadmap for digitisation in financial services. While short and medium term challenges remain, digitisation will be a key enabler for India to achieve its forecasted 7.6% GDP growth in 2019-20 FY, putting it ahead of its BRICS counterparts.

Cybersecurity poses a significant threat to this roadmap. IT and operations executives at financial institutions should instil a discipline and culture of security while mindfully enabling the enterprise with new digital capabilities and customer services.

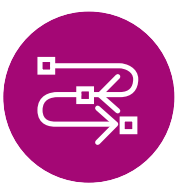
SWIFT users should remain vigilant, asking themselves five key questions and continuing to leverage tools, services and intelligence provided by the SWIFT CSP. SWIFT is committed to supporting our users in responding to persistent and sophisticated threats.

For more information refer to www.swift.com/csp and contact us at **csp.apac@swift.com**.

Are you aware how cyber threats are evolving?

Have you secured your infrastructure?

Do you have the right screening & reconciliation tools in place?



Is the channel securely integrated with enterprise systems?

Do you have the capacity to respond?

References

1. "2018 Cybersecurity Market Report", cybersecurityventures.com, April 2019
2. "Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19", ey.com, April 2019
3. "CERT India Annual Reports", cert-in.org.in, May 2019
4. "Emerging trends and challenges in cyber security", ReBIT, April 2019
5. "IT Key Metrics Data 2018: Key IT Security Measures: By Industry", gartner.com, 2018
6. FIBAC Productivity Survey 2016, 2017 and 2018 using RBI data and BCG analysis
7. "Three years on from Bangladesh, Tackling the adversaries", SWIFT ISAC Report, April 2019
8. "Data breaches affect stock performance in the long run, study finds", ZDNet, September 2018
9. "Assessing Cybersecurity Counterparty Risk, A Getting Started Guide", swift.com, January 2019
10. "World Economic Situation and Prospects 2019", unctad.org, January 2019
11. "The heightened threat of cyber attacks is fuelling payment losses – how should your business respond?", ey.com, April 2018
12. "Cyber attacks becoming more frequent in India", Hindustan Times, November 2018
13. "Smaller banks more vulnerable to cyber attacks: Experts", Business Line, August 2018
14. IT spending by Indian banks to reach $9 bn in 2017: Gartner", Business Standard, November 2017

About SWIFT

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

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, enabling them to communicate securely and exchange standardised financial messages in a reliable way. SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. Within the Programme, SWIFT has established an information sharing initiative and created a dedicated Customer Security Intelligence team, bringing together a strong group of IT and cyber experts.

The team undertakes forensic investigations on security incidents within customer premises related to SWIFT products and services; the related intelligence is published in a readily readable and searchable format in the 'SWIFT Information Sharing and Analysis Centre' (SWIFT ISAC) a global portal which is available to the SWIFT community. By feeding back this intelligence in anonymised form to the wider community, SWIFT aims to help prevent future frauds in customer environments.

SWIFT Avenue Adele 1,
B-1310 La Hulpe, Belgium
Web: swift.com
LinkedIn: linkedin.com/company/swift
Twitter: twitter.com/swiftcommunity

About BCG

Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not-for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries.

Web: bcg.com
LinkedIn: linkedin.com/company/boston-consulting-group
Twitter: twitter.com/BCG