

**ABUSE OF PAYMENT SYSTEMS IN FRAUD,
MONEY LAUNDERING, AND OTHER FINANCIAL CRIMES**

Financial criminals continue to abuse different payment systems by committing fraud, money laundering, and other crimes. Despite hefty fines imposed by regulators on prominent banks and financial institutions, criminal monies continue to flow through banks and payment operators. This session introduces ways to safeguard against the abuse of payment platforms, and identifies key areas to watch for when selecting a type of payment platform.

ANDREW KOH, CRMA, MSRM, MSGF
Deputy Chief Manager, Risk Control
China Construction Bank Corporation
Singapore

Andrew Koh is a notable thought leader, as well as a risk, fraud, and governance expert with more than 25 years of working experience in the banking, finance, credit card, and payment sectors. He has worked in credit, market, operational, regulatory, sovereign, portfolio, and integrated risk management roles, along with cross-functional roles in audit, compliance, fraud, and technology risk management. As a recognized speaker, expert panelist, moderator, and adviser, Andrew has presented to board members, directors, C-suite executives, and industry experts from central banks, government entities, financial institutions, and major corporations. He has also written a series of articles for *StrategicRISK*, an award-winning risk management magazine.

“Association of Certified Fraud Examiners,” “Certified Fraud Examiner,” “CFE,” “ACFE,” and the ACFE Logo are trademarks owned by the Association of Certified Fraud Examiners, Inc. The contents of this paper may not be transmitted, republished, modified, reproduced, distributed, copied, or sold without the prior consent of the author.

NOTES

Introduction

Financial criminals continue to abuse different payment systems by committing fraud, money laundering, and other crimes. While these have led to record-high fines imposed by regulators on prominent banks and financial institutions, the latest financial crime statistics show that crime proceeds continue to flow through banks and payment operators. This is further compounded by the rise in new digital and mobile payment technologies, which pose new threats and vulnerabilities to existing payment systems.

These developments create the need to safeguard and restore public trust in preventing the abuse of payment platforms, and to identify the six key areas we should watch for when selecting a type of payment platform for our organisations or customers.

1. Actionable and Effective Controls to Manage Frauds, ML, and Other Financial Crimes

When I was asked by the senior management of a financial institution to set up a fraud prevention framework, my first thought was to start looking for controls that are actionable, effective, and acceptable by all stakeholders, including management and the board. In short, the controls have to be known and relatively easy to understand and implement.

At that time, I was in charge of client onboarding and performing *Know-Your-Customer* (KYC) and *Anti-Money Laundering* (AML) activities. Naturally, the first control identified was *customer due diligence* (CDD), covering onboarding of clients and content providers prior to signing up mobile and digital payment services. These included *do-not-board* clients engaging in illegal activities; setting minimum requirements to include the clients' names, addresses, and bank account details; conducting business and credit searches; and collecting multiple screenshots of

NOTES

online content that e-commerce merchants are offering. If the potential clients' backgrounds still remain uncertain after the initial CDD process, then the stakeholders should carry out *enhanced* CDD to actively trace and ultimately verify the authenticity of the clients' backgrounds and wealth by requesting additional documents, such as related parties' background information, banking information, and related business dealings.

Also, *anti-money laundering rules* need to be applied to entire end-to-end business transactions, and all beneficial ownerships need to be identified. Whether one is trying to comply with the Sarbanes-Oxley Act (SOX) or the Wolfsberg Group principles (WG), it is imperative for all stakeholders to determine their clients' source of money and who ultimately owns the funds; filter out potential suspects on sanction lists; and escalate issues, such as *politically exposed persons* (PEPs), to senior management and the board for approval and oversight.

Risk monitoring of suspicious and unusual transactions on merchants, end users, and purchasers should also be in place. It is important to develop an intrinsic *understanding of root causes* so as to effectively filter out false positives and focus on genuine cases. It is also important to report all suspicious and unusual transactions relating to merchants to senior management, boards, and regulatory authorities, as KYC and AML processes might not be able to effectively identify potential terrorist financing and tax evasion activities because payment system players may not have the full information or the resources to effectively evaluate these potential risks.

It is important that all stakeholders actively engage in *industry collaboration* and *information sharing* platforms, and participate in informal working groups to discuss

NOTES

practical issues across different industries. These exchanges of knowledge and intelligence enable stakeholders to gain invaluable insights into the issues facing the affected institutions and to discuss possible solutions already formulated by other institutions. This also helps reduce the cost of information searches, and helps participants generate lists of actionable solutions gathered from other industry players in order to address similar issues within their institution.

Additionally, there are issues surrounding *commercial considerations*. There are commercial credit card rules that favour (1) merchants, who can sign-up just once to transact with global credit card holders; and (2) consumers, who can request refunds from merchants who sold them the goods or services and initiate the charge-back processes from banks.

2. How to Analyse Transaction Patterns to Detect Financial Crimes and Payment Fraud

Go beyond the minimum regulatory requirements, and establish a clear objective for why you and your institutions want to monitor transactions. Obviously, you want to detect whether any fraudulent activities are actually taking place, and whether payments are coming from illicit sources or going to questionable destinations.

Firstly, be aware of *phishing websites*. Sometimes these sites look better than the real ones, and there are *a lot* of bogus websites. There are software products that can be used to identify the authenticity of merchants' websites; financial institution management should always insist that merchants update their websites' URLs, as these can easily be changed the moment the institution onboards them. Many merchants have been known to change their URLs without notifying payment operators or banks. In some

NOTES

cases, merchants' websites redirect users to non-core business websites in an attempt to circumvent business controls and generate additional revenue.

Secondly, transactions during the holiday season generate big business for merchants, which can also generate potential big business opportunities for illicit transactions under the guise of high-volume payments. It is important for stakeholders performing transaction monitoring to ensure that the merchant's transactions match the nature of the merchant's business. For example, if a merchant is in the textile business, the merchant's transactions should not include payments from unrelated parties, such as oil businesses.

Thirdly, the *cancellation of major events*, such as pop concerts, involves large volumes of refunds, as well as cancellations flowing through consumers, merchants, banks, and payment operators. All stakeholders need to have criteria in place to identify any possibility of processing errors taking place in these transactional flows. Common situations to watch out for include (1) the slowness in ticket cancellations and who benefits from it; and (2) whether the amount refunded is less than the payments received and, if so, who has possession of the money that was not refunded.

3. Effective Use of Fraud Filter Rules to Sift Out False Positives

I cannot overemphasise the importance of *establishing effective transaction filter rules* to sift out false positives. These rules enable institutions to allocate full resources for investigating real cases. Otherwise, all the stakeholders will be sent on wild goose chases, using limited resources to go after unlimited false positives.

NOTES

If you have experience in engaging with your technology team or data analytics team, you know that they want some form of filter rules from you in order for them to assess the scope of the work and assign the relevant resources to carry out these requests. Then, of course, they want to know what the main objectives are for conducting the work.

Even after you have a set of filter rules in place and have implemented them, remember to *review the filter rules* to match the organisation's changing risk profiles.

Organisations grow their businesses organically or through mergers and acquisitions. So each time an organisation expands into a new business line or acquires existing customers, its risk profile changes, and it's your job to make sure these changes are not significant enough to warrant changes to the existing filter rules.

So, assuming you have transactional filter rules, sifted out the false positives, and identified the potential real cases, what is the next step? The next issue is whether the organisation has *effective risk and fraud governance* in place, and has written policies on the roles and responsibilities of relevant stakeholders on how they should be assuming responsibilities in discharging its fraud fighting roles. For instance, (1) the compliance team informs regulators and police; (2) the fraud team does ground investigation work; (3) the risk management team performs transaction monitoring; and (4) the internal audit team reports to management and the board.

4. How Should an Institution Operating in Several Countries Protect Its Operations Against Cross-Border Fraudulent Activities Through Its Services?

I vividly recall some memories of my discussions with the World Bank representatives on how they formulate policies and frameworks across different continents and

NOTES

jurisdictions. That is, organisations operating global business models need to *establish a baseline policy and procedural framework* to manage their operations.

The key purpose of setting up baseline policies and procedures is to capture potential fraudulent activities flowing from one country to another country that passes through the institution’s network and offices, which can effectively identify the beneficial owners who are handling the key aspects of these transactions, their delegated authorities they can operate, and whether potential fraudulent acts are identified. What this means is for policy makers to create a list of “must-haves,” driven by regulatory and compliance requirements across each country in which it operates. Procedures and processes need to be formulated around these must-haves in the specific countries in which they are conducting business, and also capture the key aspects of these rules and regulations at the group policies and procedures.

Policy makers can then enforce their baseline policies across their global operations by appointing fraud risk champions stationed in each country where the organisation operates, and with direct reporting to global headquarters. These fraud champions serve to detect potential areas of fraud issues and incidents to allow for quick decision-making and solutions to be implemented. After establishing group baseline policies, each country’s office can then proceed to tailor *specific policies and procedures* based on its specific regulatory business and compliance requirements. These approaches have been effective in supporting multinational corporations, banks, and global insurance companies.

NOTES

5. The Rise in New Fraud Threats from Alternative Payment Systems—Wallets, Cryptocurrencies, Mobile Payments

There are three key drivers to look for with regards to managing the rise in new fraud threats, especially from alternative payment systems, as these use advanced technologies that institutions' security policies and procedures might not have kept pace with.

Firstly, companies' pace and intensity on *innovation* investments far exceed their *governance, risk, and compliance* (GRC) resources. Almost everyone I know who works on the business side of an institution supports innovation more than they support governance, risk management, or compliance. The simple reason is that innovation helps firms produce more revenue and profits, whereas GRC is often deemed as a cost centre and nonprofit-generating area.

So, these innovations are, in fact, exposing institutions to fraud threats, which might end up compromising the security and integrity of their products and services offerings to their clients. The recent software manipulations on certain Volkswagen diesel engine cars to pass emission testing and standards are a case in point, whereby the entire business and reputation of the German car manufacturer are put to the test, fuelled by global regulators' ongoing investigations, growing public anger, and mistrusts.

Secondly, there's currently a complete lack of knowledge and understanding of how alternative payment systems are designed and work. These systems use advanced technologies, such as blockchains, cryptographic keys, and application programming interfaces (APIs), as opposed to the traditional payment systems, which still use 1990s encryption, end-point securities, and software codes. The

security and risk management team needs to be re-educated to further develop its knowledge and understanding of how these advanced technologies work before it is able to propose security and risk solutions to manage their networks and devices.

Thirdly, stakeholders are still figuring out how to secure codes to prevent abuse and hacking in alternative payment systems. This is because the mobile devices used most often by users are prone to malware attacks, and the lack of user awareness to secure their devices. These are further compounded by the lack of expertise within the industry to support the prevention of abuse to the payment system.

6. Challenges in Adopting Advanced Payment Technologies and Best Payment Practices

All stakeholders need to be very *clear on corporate objectives* in using advanced technologies and adopting global payment practices. Advanced technologies can either help or hinder business operations, based on users' understanding and requirements, as well as development teams and management who support the initiatives. Any deviations from the original objectives need to be proposed, discussed, and approved by senior management and the board in order to consistently align stakeholders with corporate objectives.

However, global, advanced best-payment practices may not be effective in certain countries. For example, in India, credit card rules may not be effectively enforceable, cash is widely used, and other payment alternatives are the minority.

In addition, there is an issue of managing *high set-up and monitoring costs* in using advanced payment systems using best practices. Organisations need to conduct a cost-benefit

NOTES

analysis to justify the use of advanced technologies and best practices. *Dollars* and *common sense* tend to speak louder in these areas.

Last, but not least, one has to be an effective communicator, as the decision-makers are often the people running the business. In institutions in which I have and continue to work, I always emphasize that the messages used in communicating must make business sense and carry a specific agenda to be discussed and approved. The only problem is how to make it work.

Conclusion

The abuse of different payment systems by committing fraud, money laundering, and other financial crimes have been rising in recent years. This paper has addressed some of these issues by highlighting the key areas that needed to be put in place to reduce and protect institutions from further abuse.

We must remember that our ultimate objective in addressing these issues is to enable all stakeholders to provide secure and safe products and services to their customers.

Useful References

Andreas Cremer, “Germany Investigates VW’s Ex-Boss over Fraud Allegations”, Reuters (September 29, 2015), www.reuters.com/article/2015/09/28/us-volkswagen-emissions-idUSKCN0RP14U20150928.

Andrew Koh, “Rethinking Enterprise Risk Management: A New Educational Series Looking at Practical Ideas for Managing a Variety of Risks”, *StrategicRISK*, Asia edition, Issue 5 (September 2014).

Andrew Koh, “Rethinking Enterprise Risk Management: Our Educational Series Examines Emerging Risks and Scenario Analysis”, *StrategicRISK*, Asia edition, Issue 6, (January 2015).

Bank for International Settlements, *Sound Management of Risks Related to Money Laundering and Financing of Terrorism*, (January 2014), www.bis.org/publ/bcbs275.pdf.

FICO® Falcon® Fraud Manager for Debit and Credit Card, www.fico.com/en/wp-content/secure_upload/Falcon_Debit_Credit_2909PS.pdf.

John C. Mallery, “Models of Escalation and De-escalation in Cyber Conflict”, Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology presentation at the 2011 Workshop on Cyber Security and Global Affairs, Budapest, Hungary, May 31–June 2, 2011. Version: 3/29/2012 11:04 AM.

PwC, “Global Economic Crime Survey 2014”, www.pwc.com/crimesurvey.

The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiners, *Managing the Business Risk of Fraud: A Practical Guide* (2015), www.acfe.com/uploadedFiles/ACFE_Website/Content/documents/managing-business-risk.pdf.

Monetary Authority of Singapore, *Anti-Money Laundering / Countering the Financing of Terrorism*, www.mas.gov.sg/Regulations-and-Financial-Stability/Anti-Money-Laundering-Countering-The-Financing-Of-

NOTES

[Terrorism-And-Targeted-Financial-Sanctions/Anti-Money-Laundering-and-Countering-the-Financing-of-Terrorism.aspx](#).

The Wolfsberg Group, *Wolfsberg Standards*,
www.wolfsberg-principles.com/standards.html.

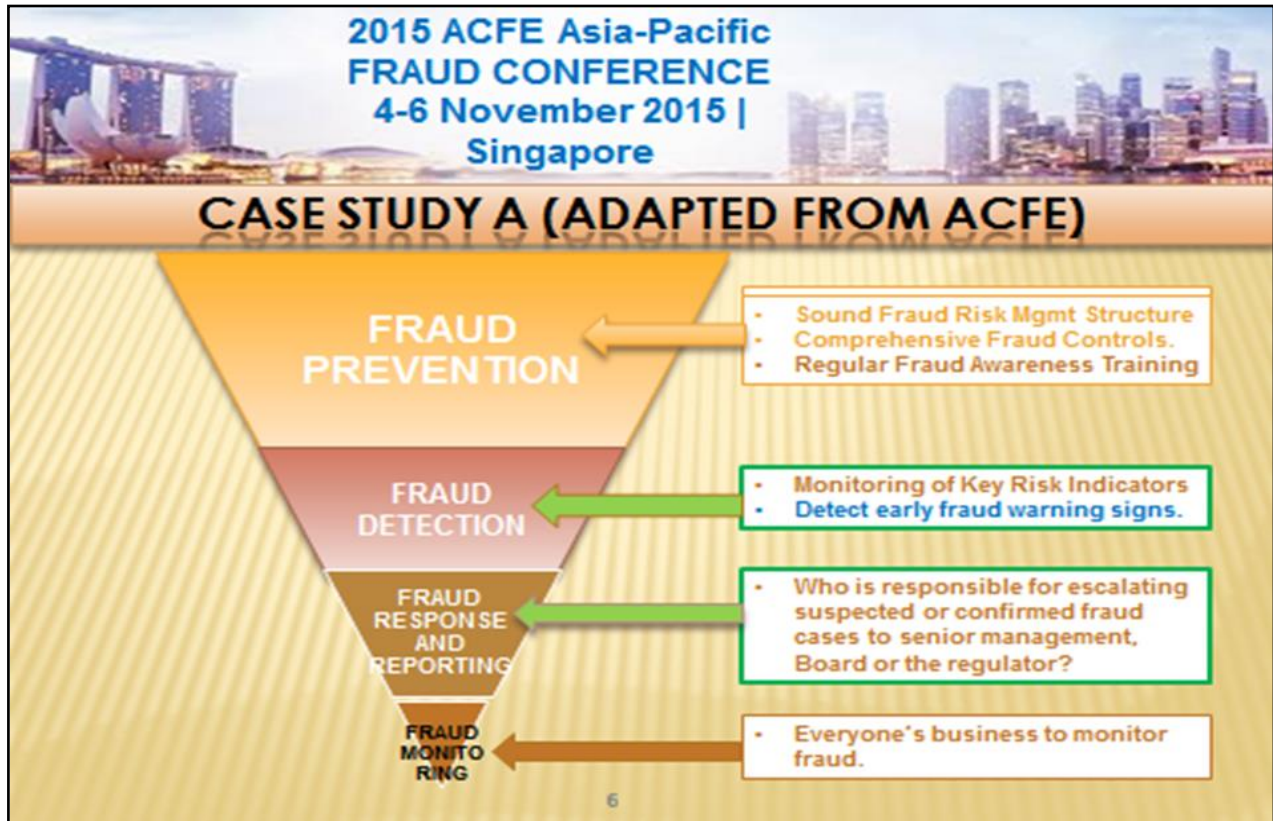
Verizon, *2015 Data Breach Investigations Report*,
www.verizonenterprise.com/DBIR/2015.

Wikipedia, Sarbanes–Oxley Act entry,
en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act.

NOTES

CASE STUDY A

How one financial institution created a risk-based fraud policy to effectively fight against digital payment abuse



CASE STUDY B

How an FI set up specialised fraud teams to detect and address illicit financial activities and payment fraud issues



**2015 ACFE Asia-Pacific
FRAUD CONFERENCE
4-6 November 2015 |
Singapore**


CASE STUDY B

A good fraud team should comprise of the following qualities:

- **Be very familiar with product design, rules and processes.**
- **Be very familiar with police investigation procedures**
- **Ready to be called into action 24/7 anytime, anywhere.**
- **Dedicated and experienced staff with “never-say-die” attitude.**
- **A few small teams are better than one big team.**
- **Establish and to record a comprehensive audit trail supported with credible evidences.**

CASE STUDY C

How data analytics can be used to sift out false positives



**2015 ACFE Asia-Pacific
FRAUD CONFERENCE
4-6 November 2015 | Singapore**

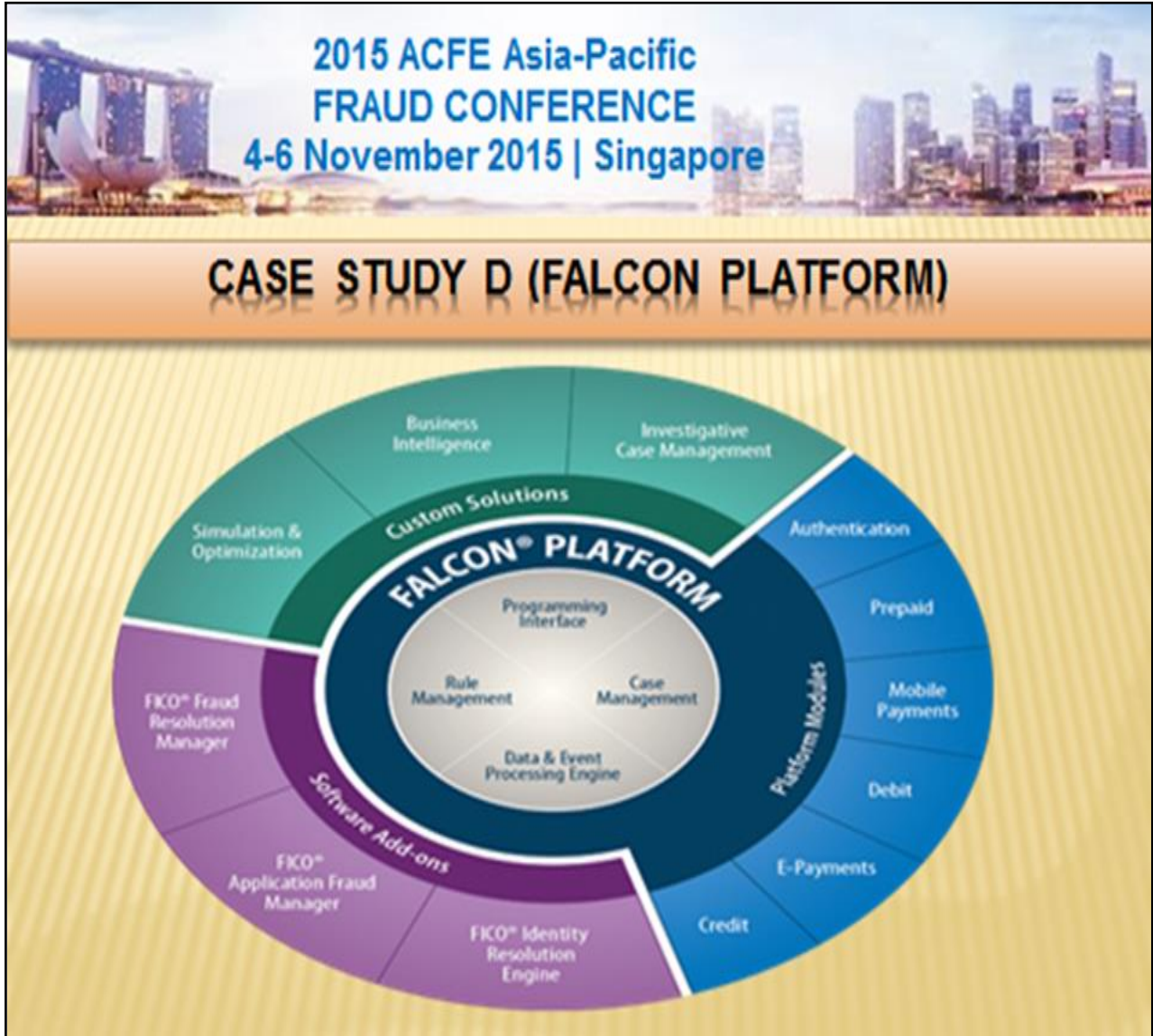
CASE STUDY C

In the case of duplicate e-payments, data analytics can help to remove the most-occurring false positives such as :

- **Remove voided checks / e-payments**
- **Remove cancelled invoices**
- **Reposting of an invoice after removing it.**
- **Remove cancelled checks / e-payments**
- **Remove intercompany account**
- **Remove of credit value invoices (requires reconciliation)**

CASE STUDY D

How a major banking group uses a technology platform to monitor its global transactional activities



CASE STUDY E

What are the new fraud threats from alternative e-payment systems?

**2015 ACFE Asia-Pacific
FRAUD CONFERENCE
4-6 November 2015 | Singapore**

CASE STUDY E

NEW FRAUD THREATS

NEW THREAT LANDSCAPE

CASE STUDY E

Threat Actors And Capabilities

Threat Actors	Motive	Targets	Means	Resources
<i>Nation States During War Time</i>	Political	Military, intelligence, infrastructure, espionage, reconnaissance, influence operations, world orders	Intelligence, military, broad private sector	Fully mobilized, multi-spectrum
<i>Nation States During Peace Time</i>	Political	Espionage, reconnaissance, influence operations, world orders	Intelligence, military, leverages criminal enterprises or black markets	High, multi-spectrum, variable skill sets below major cyber powers
<i>Terrorists, Insurgents</i>	Political	Infrastructure, extortion	Leverage black markets?	Limited, low expertise
<i>Political Activists or Parties</i>	Political	Political outcomes	Outsourcing?	Limited, low expertise
<i>Black Markets For Cyber Crime</i>	Financial	Hijacked resources, fraud, theft, IP theft, illicit content, scams, crime for hire	Tools, exploits, platforms, data, expertise, planning	Mobilizes cyber crime networks
<i>Criminal Enterprises</i>	Financial		Reconnaissance, planning, diverse expertise	Professional, low end multi-spectrum, leverage of black markets
<i>Small Scale Criminals</i>	Financial		Leverages black markets	Low, mostly reliant on black markets
<i>Rogue Enterprises</i>	Financial	IP theft, influence on sectoral issues	Outsourcing to criminal enterprises?	Sectoral expertise, funding, organization

John C. Mallery
7
MIT CSAIL

CASE STUDY F

How a financial institution failed to successfully set up an AML system to monitor payment transactions

