Wall street fintech club (WSFC)

Fraud Workshop

Shan Xu

PwC's Financial Crime Unit

April 14th, 2017

Please contact shan.xu@pwc.com for the full deck

pwc

Fraud Risk Landscape

Stark Realities of Fraud

FBI Issued Warning: Rising threat of wire transfer fraud through business email compromise schemes[1]

Hack on SWIFT system costs $101M[3]

Hackers breached Bangladesh Central Bank's computer systems and used its Swift messaging system to submit 35 payment requests to the Federal Reserve Bank of New York. The New York Fed transferred $101 million to fictitious accounts at Rizal Commercial Banking Corporation (RCBC) in the Philippines and another bank in Sri Lanka before it became suspicious and denied the remaining 30 requests

Total financial losses *stemming from* ***ID theft*** *estimated to be* ***$50 Million***[6]

FBI: Public & Private Sector Officials **at Risk for Social Engineering** to Gain Access to Victims' Data[8]

Citi may face $827M charge over AIB Rouge Trader Suit[14]

Card fraud costs the US billions each year

Payment card fraud cost banks $7.9B, an increase in almost 60% from five years earlier[9]

Deutsche Bank AG is investigating a series of trades that may have improperly generated over **$30 million dollars in fraudulent personal profits**[15]

J.P. Morgan Advisor Admits Stealing $20M From Clients[2]

A former Capital One Financial Corp. analyst was ordered to pay $13.5 million in sanctions for insider trading[4]

Natixis Funding Corp. and Société Générale agreed to a settlement of $56 million for charges of defrauding state and local governments and nonprofits throughout the US in municipal bond derivative transactions[5]

Wells Fargo will pay $190 million for pushing customers into fee-generating accounts they never requested[7]

FINRA proposes rule with SEC to protect seniors and other vulnerable adults from financial exploitation[10]

Total financial losses *stemming from* ***check fraud*** *estimated to be* ***$12B*** *for U.S. Banks*[12]

SunTrust executive ordered to pay **$1.9M** for **falsifying loan documents** and committing **mortgage fraud**[11]

Goldman Sachs reaches a $5.1B deal with US authorities over charges that it used fraudulent marketing material to sell mortgage bonds before the financial crisis[13]

Current Fraud Schemes

- Identity Theft
- Account Takeover/ Compromise
- Social Engineering (High Profile Client/ Senior Management)
- Misrepresentation of P&L / Valuation / Performance
- Dormant Account Abuse
- Abuse of Position (UT)
- Ponzi Scheme
- Collusion
- Pump & Dump
- Overstatement of Fees or Expenses

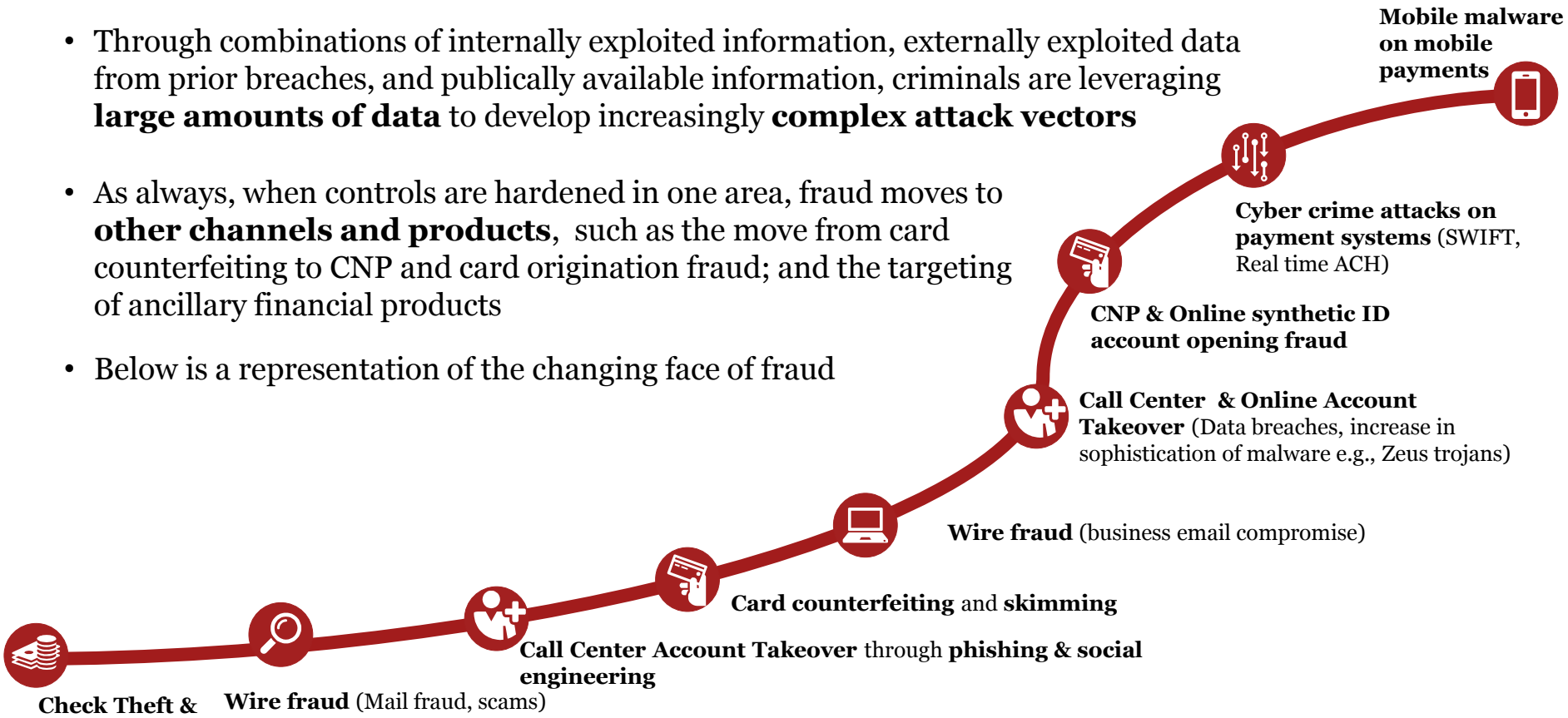
Emerging Fraud Schemes

- Business Email Compromise
- Social Media Account Compromise
- Phishing
- Elderly Abuse
- P2P (Peer-to-Peer) Payment Fraud
- M2M (Machine-to-Machine) Attack
- Client VPN Compromise
- Mobile Payments Fraud
- Brand Misrepresentation
- Synthetic Identity Theft

1. See Cyber Fraudsters Reap $2.3 Billion Through Wire Transfer, 2. See Advisor Must Pay, 3. See SWIFT Related Heist Who's To Blame, 4. See US SEC Capital One Insider Trading, 5. See Natixis & Société Générale Settle Municipal Bond Fraud Charges, 6. See Identity Theft Prevention, 7. See Wells Fargo Settlement, 8. See FBI Warns of Dramatic Increase in Business E-Mail Scams , 9. See Card Fraud Costs the US Billions Each Year — Here's What Card Networks are Doing About It, 10. See FINRA Files Rule Proposal with SEC to Protect Seniors and Other Vulnerable Adults from Financial Exploitation, 11. See Big Bank Headed to Prison for Mortgage Fraud, 12. See Check Fraud Remains Major Threat, 13. See Goldman Sachs in $5.1b deal over bond mis-selling, 14, Options Broker Charged in Pump & Dump Scheme, 15. See Deutsche Bank Internally Probes Dubious Trades

The Evolution of the Fraud Landscape

- Over the years fraudsters and fraud schemes have evolved in line with the changing face of financial services – from traditional banking channels to **digital product** offerings and platforms - with fraudsters continuing to seek out and target the path of least resistance, exploiting control vulnerabilities and less secured channels, such as mobile and call center
- Through combinations of internally exploited information, externally exploited data from prior breaches, and publically available information, criminals are leveraging **large amounts of data** to develop increasingly **complex attack vectors**
- As always, when controls are hardened in one area, fraud moves to **other channels and products**, such as the move from card counterfeiting to CNP and card origination fraud; and the targeting of ancillary financial products
- Below is a representation of the changing face of fraud



Leading Approaches

Past project examples

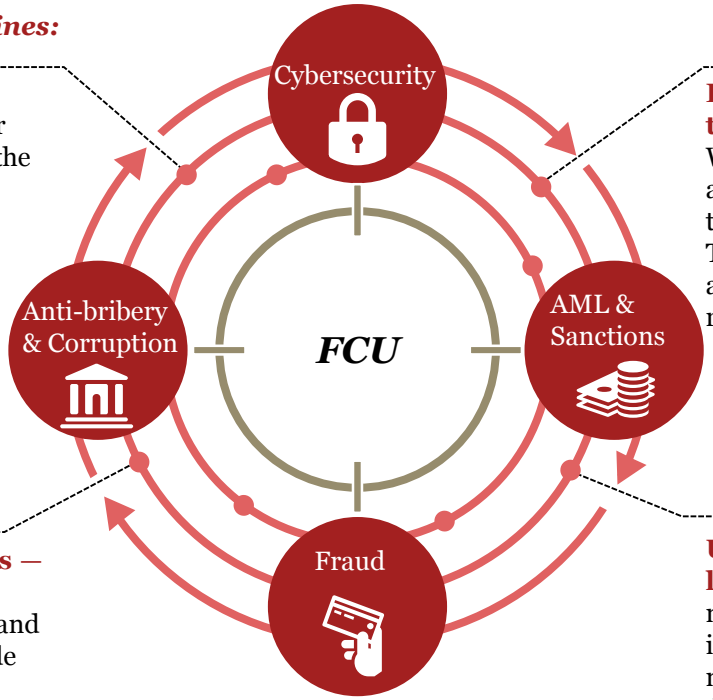
PwC's Financial Crimes Unit (FCU)

Financial crime is a major threat to the safety and soundness of financial institutions worldwide. As a result, it has become a top agenda item for The White House, Regulators, and both the Boards and CEOs of major financial institutions.

PwC's Financial Services FCU provides a holistic and integrated approach to navigating financial crimes. Four key areas collectively form the foundation for our financial crimes approach:
1) Cybersecurity, 2) Anti-Money Laundering (AML) and Sanctions, 3) Fraud, and 4) Anti-Bribery and Corruption.

Our team and our approach combines:

Deep subject matter expertise and industry experience — Led by Former Deputy Director of the FBI, Sean Joyce, the FCU is comprised of more than 300 professionals with experience as former risk managers, forensic investigators, regulators, law-enforcement officials, national security officials and seasoned consultants.



Innovative and efficiency gaining tools—
We have a repository of tools and accelerators to help our clients address their various financial crime challenges. These include threat libraries, risk assessment framework, policy frameworks, rules libraries and models.

Strategic alliances with key vendors — Our numerous relationships with key vendors enhance engagement efficiency and technology implementation; these include Actimize, Oracle, Guardian Analytics, ThetaRay, Tanium, IronNet, FireEye and Securonix, among others,

Unparalleled knowledge of industry leading practices —PwC has assisted many of the largest global, US and regional institutions across the banking & capital markets, asset management and credit/ debit cards industries to fully address the complex business issue of financial crimes from board-level advice and strategy through execution.

For further details, please visit: PwC Financial Crimes Unit Website

Large global card issuer and retail bank

Client issue	The client experienced a significant increase in Fraud Applications. The client believed that their detection strategies were robust and they needed more people to review and disposition fraud alerts.
Challenges	Client onboarding processes were not well understood. Several anti-fraud point solutions were outdated and their rules and thresholds were not known. There were unclear roles and responsibilities between the first and second lines of defense and teams work in silo. Data points were available not being utilized.
What we did	PwC analyzed the client's processes and controls across the customer life cycle and performed data analysis to determine actual root causes of confirmed frauds and developed recommendations on fraud controls and implementation roadmap. We interviewed and analyzed the skillsets of the fraud teams and help design the future state fraud organization.
Impact	PwC developed several recommendations to improve the client's detection strategies including proposed new point solutions, update to their detection rules and revamp of their data and technology infrastructure to move to a more real-time detection. The proposed detection strategies would detect 60% more frauds.