Executive summary:
The evolution of borderless financial crime

The financial services industry is facing an emerging era of borderless, networked financial crime threats. Is the industry ready?

<table>
<thead>
<tr>
<th>The emerging threat</th>
<th>• A new era of increasingly complex, coordinated, global financial crime attacks by professionals who are highly networked, well informed, well organized and borderless</th>
</tr>
</thead>
<tbody>
<tr>
<td>The current gap</td>
<td>• Structured attacks that fly under the radar of siloed organizations and technologies to exploit organizational boundaries and blind spots</td>
</tr>
<tr>
<td>The necessary response</td>
<td>• Connect people, data and technologies pervasively to promote fully informed, client-centric risk assessment and surveillance across organizational boundaries</td>
</tr>
</tbody>
</table>
Attacks consist of multiple phases executed by a borderless network of specialists:

- Hackers quietly and systematically probe and map financial crime controls of banks and third-party processors by using a combination of modalities, including ID theft/takeover, denial of service (DoS), and device/network compromise.
- Once vulnerabilities and organizational blind spots have been mapped, criminals rapidly launch large, multi-stage, cross-channel attacks via card fraud, money transfer fraud, first-party fraud and, increasingly, insider fraud.
- Kingpins launder funds through the global banking system.
- Despite having robust controls, leading financial institutions are victimized due to weak links outside of their controls, such as payment network members and third-party service providers.

The facts

- Top threats as ranked by deposit fraud executives\(^1\)
  - Debit card fraud
  - Cross-channel attacks
  - Organized rings
- **Eighty-two percent** of fraud goes undetected until client reported.\(^2\)
- **Seventy-seven percent** of firms have been victims of external attacks in the past year.\(^3\)
- **Sixty-six percent** of firms have no formal security architecture framework.\(^3\)
- **Eighty-four percent** of fraud executives say current controls fail to keep up with evolving threats, struggle to work across channels and/or are difficult to integrate with other applications and tools.\(^2\)
Recent case study

Professionalization of financial crime is happening today. Large US and foreign financial institutions have been victimized in recent months.

The storyline

- A Middle Eastern bank relies on an offshore card processor to handle stored-value transactions.
- A global network of hackers conducts a surgical penetration of the offshore processor, eliminating withdrawal limits and manipulating stored-value balances on accounts. The penetration enables the withdrawal of unlimited amounts of cash. The compromise goes undetected.
- Criminal “casher” rings in dozens of cities conduct rapid, synchronized “unlimited operations” to withdraw large sums of cash from ATMs of large banks.
- Funds are laundered by kingpins through structuring, layering and purchasing high-value goods that are subsequently transported offshore.

ATM withdrawal activity over five hours by one casher in Manhattan, Feb 19, 2013. Selected large withdrawals are highlighted.⁴

1. 4:11 p.m., $4,015
2. 5:10 p.m., $2,409
3. 5:28 p.m., $2,409
4. 6:17 p.m., $2,409
5. 6:24 p.m., $2,409
6. 6:43 p.m., $2,409
7. 8:55 p.m., $2,409
8. 9:24 p.m., $5,621
9. 9:55 p.m., $4,015
The facts

- $45m stolen in two ATM-withdrawal sprees on Dec. 22, 2012, and Feb. 19-20, 2013, including $2.8m stolen from ATMs in Manhattan over a 10-hour period February 19-20, 2013
- 27 countries in which ATMs were raided
- 17 prepaid credit card accounts used
- 40,500 total ATM withdrawals, including 2,904 withdrawals in Manhattan
# Key takeaways

Large financial institutions need to take measures now to prevent the growth of this new era of borderless financial crime.

## Were the banks responsible?
- Financial institutions involved generally maintained effective, FFIEC-compliant control environments. Neither the issuing banks nor the ATM owners were compromised.
- Despite having effective internal controls, these institutions fell victim to security vulnerabilities of their third-party card processors.
- The contracting institutions are responsible for understanding, assessing, confirming compliance and monitoring the control environments of their outsourced service providers.
- A recent McKinsey article summarized the position of regulators: “Activities can be outsourced, but responsibility can’t.”

## How did criminals gain access?
- Evidence suggests that access was gained through Advanced Persistent Threats (APTs), a combination of coordinated attack vectors, including hacking, phishing, social engineering and denial of service.
- Insiders employed by third-party processors may have conspired with the professional criminals to gain access.

## Which controls were missing?
- The issuing banks may not have consistently followed vendor management best practices, such as security audits, risk assessments and penetration testing.
- Banks and third-party processors were slow to detect and respond to the massive cash-out.
- Robust, risk-based card fraud transaction monitoring must be in place, but that is not enough.
- The ability to raise limits on withdrawals should be a system-enforced permission granted to only a limited set of trusted administrative accounts. Thorough background checks, approval processes and activity monitoring must be in place for these accounts.
- Changes made to transactional systems should require a systematic approval process, including segregation of duties to enforce security policy.
Implement practical preventive measures

Irrespective of who is at fault, large global financial institutions risk financial, reputational and customer satisfaction damage from borderless attacks. Institutions should augment controls, including:

<table>
<thead>
<tr>
<th>Formalize the organization’s security architecture framework</th>
<th>Conduct supplier risk and security management reviews</th>
<th>Enhance monitoring of card account, transactional activity and network activity</th>
<th>Develop intelligence and information-sharing capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Link information security architecture to business strategy and risk appetite in order to support growth, innovation and optimization, while enhancing protection and governance</td>
<td>• Consistently apply strong supplier risk and security management processes</td>
<td>• Build real-time, detailed behavior profiles for each device, ATM and relationship</td>
<td>• Implement a dedicated Financial Crime Intelligence function to monitor external fraud alert networks and internal sources with the objective of anticipating and preventing loss from emerging financial crime patterns</td>
</tr>
<tr>
<td>• Implement a highly interconnected architecture across the institution and its third-party processors to give monitoring systems and fraud/security analysts a complete, global relationship-level picture of all activity</td>
<td>• Include initial service provider due diligence in robust security reviews</td>
<td>• Automatically apply interdiction controls based on anomalous behavior and link analysis</td>
<td>• Proactively monitor patterns of fraud, social engineering and link analysis</td>
</tr>
<tr>
<td>• Conduct ongoing risk-based reviews of security controls, verifying that each employee has only the absolute minimum-required access and ensure systematically enforced segregation of duties</td>
<td>• Perform annual, independent, risk-based reviews of all service providers who handle transactional or customer activity to ensure they have defined and implemented effective, appropriate, consistent policies, processes and control structures to identify and adapt to emerging threats</td>
<td>• Expedite implementation of card chip-and-pin (Europay, MasterCard and Visa, or EMV) to take advantage of enhanced security features for customers who present EMV-enabled cards</td>
<td>• Implement an ongoing process to extract intelligence from all available data on signals and trends to create and implement actionable risk-mitigation strategies before attacks begin</td>
</tr>
<tr>
<td></td>
<td>• Assess the effectiveness of transaction surveillance systems to ensure mass compromise can be systematically detected and automatically stopped</td>
<td>• Assess the effectiveness of transaction surveillance systems to ensure mass compromise can be systematically detected and automatically stopped</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Review ATM configurations to identify and remove unnecessary services and ensure configurations are current</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
EY can help

For the fourth year in a row, EY has been recognized by Risk.net’s *Operational Risk & Regulation* magazine as the “best overall consultancy.” We were also recognized as the number one consultancy for fraud/financial crime prevention in the magazine’s latest report (2011).

EY has:

- A proven track record of assisting financial institutions to assess, improve, and transform their financial crimes capabilities
- A team of experienced fraud management and information security consultants, including former executives from the banking industry as well as leading software vendors
- Highly relevant experience configuring and deploying turnkey fraud, security and compliance technology solutions
- Deep banking and payments industry domain knowledge
- Knowledge and hands-on experience across the complete software development life cycle
- Experience with leading software vendors and leading analytics and decision support technologies

EY can provide:

- Assistance with assessment, strategic planning, design, and implementation of security and financial crime processes and technologies based on our extensive experience with fraud management, information security, supplier risk management, and analytics
- Guidance from our experienced global fraud management and information security practices on industry trends in key markets around the world
- Insight into global trends and practices across the financial landscape
- Flexible cost models to deliver global operational and technology solution implementations
Key contacts

To hear more about how our team can help you, please contact the following professionals:

**Ron Giammarco**  
*Partner, Financial Services*  
Ernst & Young LLP  
Renato.Giammarco@ey.com  
+1 212 773 3409

**Nik Walser**  
*Senior Manager, Financial Services*  
Ernst & Young LLP  
Nik.Walser@ey.com  
+1 212 773 5506

**David Nussenbaum**  
*Senior Manager, Financial Services*  
Ernst & Young LLP  
David.Nussenbaum@ey.com  
+1 212 773 4523
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2013 EYGM Limited
All Rights Reserved.

EYG no. CK0717
1310-1152512 NY
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, or other professional advice. Please refer to your advisors for specific advice.

ey.com

Endnotes
1. 2011 ABA Deposit Account Fraud Survey.
2. ISMG 2012 Faces of Fraud survey.
3. EY 2012 Global information security survey.