Occasional Paper

Targeting Security Threats Using Financial Intelligence

The US Experience in Public–Private Information Sharing since 9/11

David Carlisle
Targeting Security Threats Using Financial Intelligence
The US Experience in Public–Private Information Sharing since 9/11

David Carlisle
Over 180 years of independent defence and security thinking

The Royal United Services Institute is the UK’s leading independent think-tank on international defence and security. Its mission is to be an analytical, research-led global forum for informing, influencing and enhancing public debate on a safer and more stable world.

Since its foundation in 1831, RUSI has relied on its members to support its activities, sustaining its political independence for over 180 years.

London | Brussels | Nairobi | Doha | Tokyo | Washington, DC

The views expressed in this publication are those of the author(s), and do not reflect the views of RUSI or any other institution.

Published in 2016 by the Royal United Services Institute for Defence and Security Studies.

This work is licensed under a Creative Commons Attribution – Non-Commercial – No-Derivatives 4.0 International Licence. For more information, see <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

RUSI Occasional Paper, April 2016. ISSN 2397-0286 (Online).
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>v</td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td>1</td>
</tr>
<tr>
<td><strong>I. The Evolving Project of Section 314</strong></td>
<td></td>
</tr>
<tr>
<td>Laying a Foundation: The Origins and Intentions of Section 314</td>
<td>7</td>
</tr>
<tr>
<td>Fifteen Years On: Evaluating the 314 Partnership</td>
<td>12</td>
</tr>
<tr>
<td><strong>II. Section 311: Special Measures, Primary Concerns</strong></td>
<td></td>
</tr>
<tr>
<td>Laying a Foundation: The Origins and Intentions of Section 311</td>
<td>23</td>
</tr>
<tr>
<td>Section 311 Successes</td>
<td>25</td>
</tr>
<tr>
<td>Advantages of the Section 311 Approach</td>
<td>27</td>
</tr>
<tr>
<td>Disadvantages of the Section 311 Approach</td>
<td>29</td>
</tr>
<tr>
<td><strong>Conclusion and Recommendations</strong></td>
<td>31</td>
</tr>
<tr>
<td>About the Author</td>
<td>35</td>
</tr>
</tbody>
</table>
For a long time observers have believed that public–private partnership is a key tool in the effort to combat money laundering and terrorist financing. Since the founding of the Financial Action Task Force (FATF) in 1989, the interaction of the private and public sectors has been a pillar of the architecture constructed to disrupt financial crime. As David Carlisle points out in this paper, this relationship should be mutually beneficial. In the UK and elsewhere around the world, whilst a form of information sharing exists in order to meet the requirements of the FATF, the effectiveness of and satisfaction with most forms of information sharing remains low and frustrates all involved.

In order to identify best practice and inform policy-makers as they seek to enhance the domestic and international information-sharing architecture, the Centre for Financial Crime and Security Studies (CFCS) at the Royal United Services Institute (RUSI) is dedicating significant time to addressing this issue. In 2015, our information-sharing programme began with a flagship conference, Tackling Money Laundering: Towards a New Model for Information Sharing, which brought together national financial intelligence units, officials from law enforcement, prosecutors and senior figures from the financial services industry. This conference was followed up by extensive engagement with both public and private actors, and further research and events such as a series of workshops held in autumn 2015 as part of the consultation with stakeholders on an improved UK Suspicious Activity Reports regime.

In this spirit, David Carlisle’s paper illuminates an important and longstanding set of information-sharing tools from the US that are often cited as being worthy of replication. As he notes, Sections 314 and 311 of the USA PATRIOT Act help to sustain a robust, if still maturing, public–private partnership aimed at protecting the US financial system against a broad array of illicit finance threats.

Although, as this paper reveals, in reality these tools cannot yet achieve all the objectives set by policymakers, the model represents a good starting point for states in which a lack of information sharing continues to inhibit the disruption of financial crime. Of course, the paper does not suggest that the US model is the only option, nor does it necessarily suggest that such a model will be suitable for wholesale import into the UK. However, understanding the tools developed by other states and their benefits and shortcomings should provide the UK and others with a basis from which to work on developing and implementing much needed improvements.

Over the coming months, the CFCS will continue to work through the challenges that face law enforcement, policy-makers and the private sector as they seek to share information more effectively in an effort to disrupt financial crime. It hopes to develop a clear understanding of what information sharing can reasonably deliver and how information sharing can be appropriately constructed, balancing the needs of security and data privacy.

Tom Keatinge
Director, Centre for Financial Crime and Security Studies, RUSI
April 2016
Introduction

SINCE THE FOUNDING of the Financial Action Task Force (FATF) in 1989, global efforts on anti-money laundering and counter-terrorist financing (AML/CTF) have rested on the principle that co-operation between the public and private sectors is essential in generating financial intelligence (FININT). Ideally, this relationship should be mutually beneficial and iterative: governments can draw on multi-source intelligence to provide the private sector with information on criminal and terrorist typologies, thereby enhancing the ability of financial institutions to identify illicit activity among their customers and transactions. Equipped with this knowledge, financial institutions can provide government and law enforcement with detailed information about financial activity to support legal or regulatory action against specific criminal and terrorist targets.

Recently, however, a consensus has emerged in both the public and private sectors that the frequency and quality of financial information sharing is inadequate. Observers argue that governments do not supply the private sector with sufficient detail about key threats, such as terrorism, for financial institutions to generate high-quality FININT. On the other hand, private sector reporting of FININT through the traditional Suspicious Activity Reports (SARs) process is often slow and inefficient, hindering the ability of governments to act against criminals or terrorists.

For example, in December 2015, the UN Security Council responded to the threat from Daesh (also known as the Islamic State of Iraq and Syria, ISIS) by calling on member states ‘to engage with financial institutions and share information on terrorist financing (TF) risks to provide greater context for their work in identifying potential TF activity … and to promote stronger relationships between governments and the private sector in countering terrorist financing’.¹ Similarly, the FATF recently noted that for CTF efforts to succeed, ‘better [financial] information sharing is required between … the public and private sector.’² RUSI has examined the prospect for bolstering public–private information-sharing partnerships in other recent publications.³

Despite these growing calls for enhanced public–private FININT collaboration, there are substantial practical challenges. Personal data privacy requirements, the commercial and legal challenges facing financial institutions, and the anxiety of security agencies over disclosing

---

1. UN Security Council Resolution 2253, 17 December 2015, SC/12168, para. 3.
sensitive information make information sharing anything but straightforward. What is more, there are few existing examples of public–private FININT partnerships for policy-makers to refer to.

Fortunately, one relatively longstanding model for public–private information sharing does exist. Shortly after the 9/11 attacks, in October 2001, President George W Bush signed into law the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. One aim of the Act was to elevate the role of FININT in identifying and disrupting security threats. Two sections of the Act have particular relevance for promoting public–private information sharing to this end: Sections 314 and 311.

Set alongside the traditional SARs regime, Sections 314 and 311 help to sustain a robust, if still maturing, public–private partnership aimed at protecting the US financial system against a broad array of illicit finance threats.

Section 314, and specifically its sub-Sections 314(a) and (b), seeks to facilitate more rapid and fluid information sharing among the public and private sectors. On the one hand, Section 314(a) enables public–private information sharing. As implemented, under Section 314(a) law enforcement agencies can submit streamlined requests on specific investigative targets to thousands of US financial institutions simultaneously. These requests compel financial institutions to search their records for evidence of suspected criminals’ financial activity and to supply law enforcement with basic information about that activity where they identify it. The process saves law enforcement agencies valuable time and resources by allowing them to survey the US financial sector quickly for investigative leads not available elsewhere; and it provides the private sector with concrete information about individuals and entities whose transactions the security services believe warrant scrutiny.

Section 314(b), on the other hand, enables private–private information sharing. It permits US financial institutions to share with one another, on a voluntary basis and without liability for disclosure of personal data, information pertaining to customers, accounts, or transactions they suspect may be related to money laundering or terrorism. The rationale for Section 314(b)’s design is simple: when gathering information on their customers and transactions, financial institutions often have a narrow picture of events – that is, they may have insight into activity that occurs on their own books, but lack insight into the source, ultimate destination, and purpose of their customers’ activity that involves other financial institutions. The aim of Section 314(b) is to allow financial institutions to have a more well-rounded view of customers and transactions. This can help the private sector to produce higher quality SARs, which can in turn complement law enforcement investigations.

The text of the PATRIOT Act and statements of US officials point to three broad objectives for Section 314:

- Improve the quality of FININT about money laundering and terrorism available to law enforcement and regulators, in order to support legal or regulatory action against targets.
• Enhance the ability of financial institutions to make informed decisions about customers, accounts and transactions by improving the quality of information available to the private sector about money laundering and terrorism.

• Promote a culture of responsible, secure information sharing across the public and private sectors.

By most available accounts, Section 314 has improved the US’s ability to achieve these objectives since 9/11.

US implementation of Section 314, however, has not been a story of complete success. In particular, voluntary participation by financial institutions in the 314(b) programme is not widespread. Whereas a common critique of the PATRIOT Act as a whole is that it is an example of government overreach, a frequent criticism of Section 314(b) is that its provisions are not sufficiently broad, or clear, to promote widespread private sector participation. Furthermore, US financial institutions have struggled to manage the complicated and sensitive process of sharing information with their peers. This paper will examine these and other related challenges.

This paper also considers Section 311 of the PATRIOT Act, which authorises the secretary of the Treasury to require US financial institutions to gather intelligence on specific exceptional threats to the US and international financial systems. During the 1990s, US policy-makers began to view international money laundering and its attendant ills – such as terrorism, corruption, and organised crime – as significant national security threats. This view mirrored the FATF’s concurrent efforts to establish and elevate the role of international AML standards that could protect the global financial system from illicit finance threats. However, by the time of 9/11 many policy-makers recognised that the US lacked sufficient means to deter these threats and enforce the FATF’s standards.

Therefore, whereas Section 314 acts as the basis for facilitating day-to-day FININT-sharing arrangements against a potentially endless array of money laundering and terrorist-financing threats, Section 311 acts as a complementary policy tool for directing the attention of financial institutions to a smaller number of specific, high-priority threats.

As with Section 314, the text of the PATRIOT Act and the remarks of US officials suggest three broad aims against which Section 311 implementation efforts may be assessed:

• Enhance the public sector’s ability to alert financial institutions to exceptional threats.

• Facilitate the generation of targeted FININT in support of law enforcement or regulatory action against threats.

• Support US and international security objectives by disrupting the financial activity of targets.

A review of Section 311 actions taken to date suggests the US is generally able to achieve these aims. However, Section 311 rests on extremely broad powers that some countries may be reluctant to invest in their public sector agencies. Furthermore, its ability to disrupt targets’ activity rests on the significant influence of the US financial sector globally and may not be easily replicable in other jurisdictions. Despite these concerns, Section 311’s record-keeping and reporting provisions may nonetheless offer an attractive prototype for other countries seeking to enhance their FININT-collection capabilities.

Methodology, Aims and Scope

In considering Sections 314 and 311 as models for information sharing, this paper draws on existing literature, including publicly available statements from US officials and private sector representatives. It also draws on discussions held in February and March 2016 with more than half-a-dozen experts who have experience in both the public and private sectors.

The paper does not consider broader issues of concern, such as whether public–private FININT collaboration is indeed an essential pillar of international security, or whether data privacy concerns outweigh the need to share intelligence; nor does it attempt to judge the legality or prudence of specific actions taken under Sections 314 and 311. Rather, it acknowledges that the PATRIOT Act is a frequently utilised piece of legislation, and that the US will continue to refine its use of Sections 314 and 311. Furthermore, this paper acknowledges that other governments are already examining and experimenting with ways to strengthen public–private frameworks and are likely to look to the PATRIOT Act as a guide.

To this end, this paper offers an overview of the aims of US policy, an examination of the US experience in implementing Sections 314 and 311 of the PATRIOT Act, and a consideration of the advantages and disadvantages of the US approach. It also draws lessons from US experience and provides the following principles for policy-makers to consider when developing public–private information-sharing arrangements at the national or international level.

Recommendations

1. **Clarity:** To encourage private sector participation, legislation should be clear on the scope and intent of permissible information sharing and related legal protections.

2. **Consensus:** Consensus between the public and private sectors about the objectives of information-sharing arrangements and related legal provisions is necessary to achieve meaningful outcomes.

3. **Functionality:** Legislative authorisation for information sharing should be supported by robust technical mechanisms and collaborative fora that facilitate the secure and timely exchange of information.

4. **Proactive Engagement:** With appropriate data-protection safeguards in place, the private sector should be trusted to identify and share information on threats with discretion; but governments, and financial intelligence units (FIUs) in particular, should be active,
engaged guides that provide the private sector with timely and useful information about threats.

5. **Prioritisation**: Information-sharing partnerships should seek a balanced approach: they should be risk-based and directed at identifying specific high-priority threats, yet still sufficiently broad to capture a range of emerging threats.

6. **Inclusiveness**: To counter the ability of criminals to operate swiftly across the financial sector, information-sharing arrangements should aim to involve as many types of financial institutions and law enforcement agencies active in a jurisdiction as is reasonably possible.

7. **Flexibility**: Arrangements should be adaptable and open to amendment to keep pace with changing threat landscapes and evolving compliance challenges.
I. The Evolving Project of Section 314

The name given to Section 314 – ‘Cooperative Efforts to Deter Money Laundering’ – makes its intentions clear. After the 9/11 attacks, the US government sought to strengthen AML/CTF efforts by fostering close, collaborative working relationships between law enforcement bodies, regulatory agencies and financial institutions.

Sub-section 314(a) functions as a prelude – not as a substitute – to the traditional subpoena process. It allows law enforcement to share the names of specific targets of money laundering and terrorism investigations with the private sector for the purpose of rapidly generating basic information on suspects’ financial activity. In doing so, Section 314(a) aims to save time and resources when conducting investigations and sharing related information. Sub-section 314(b) is based on the premise that sharing information within the private sector is essential for financial institutions to build the complete and meaningful picture of financial activity required to produce high-quality, actionable FININT.

Before examining the strengths and limitations of the US private–public information-sharing project, it is worth considering the rationale behind the design of Section 314 and the history of its implementation.

Laying a Foundation: The Origins and Intentions of Section 314

Section 314(a)

Before 9/11, information-sharing between US law enforcement bodies, regulatory agencies, and financial institutions was often slow and inefficient. If a law enforcement investigator wanted to learn if any financial institutions had information on a specific suspect to generate investigative leads, the investigator had to make inquiries bank-by-bank, an often impractical exercise that discouraged information sharing. Where constructive information sharing for investigative leads did occur, it was ad hoc and not replicated widely. Because co-operation was infrequent, law enforcement and financial institutions did not have robust working relationships. When law enforcement did succeed in determining that a financial institution maintained an account for the suspect under investigation, by the time it had received grand jury subpoenas to request account details, the information a financial institution provided could be outdated or of little value. Financial institutions, for their part, often found the information-sharing process frustrating. For financial institutions to play a useful role in generating FININT, it is important that

6. Author’s discussions with experts, February 2016.
they understand the types of information that are valuable to government and law enforcement. Lessons learned from information sharing allow financial institutions to amend their practices and target resources appropriately. Prior to 9/11, financial institutions received little feedback from law enforcement about the outcomes of cases where they did provide assistance, and as a result they struggled to understand the utility of their role in information sharing.8

The inclusion of Section 314(a) in the PATRIOT Act was an attempt to correct this informal, inefficient dynamic. Specifically, Section 314(a) requires the secretary of the Treasury to:

> adopt regulations to encourage further cooperation among financial institutions, their regulatory authorities, and law enforcement authorities, with the specific purpose of encouraging regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected based on credible evidence of engaging in terrorist acts or money laundering activities.9

In September 2002, the Financial Crime Enforcement Network (FinCEN) – the US FIU – adopted implementing regulations for Section 314(a). The regulations allowed federal law enforcement agencies to expedite the search for financial information by providing the names of subjects in their money laundering or terrorism investigations to FinCEN, which would then distribute the requests to US financial institutions – either broadly or targeted, as appropriate – to search their account and transaction data for matches against suspect names. If financial institutions found matches, law enforcement could use that information to prompt requests for grand jury subpoenas to obtain more detailed account and transactional details.

The initial process of implementing this requirement was not straightforward. In November 2002, following negative feedback from financial institutions, FinCEN placed a moratorium on all 314(a) requests:10 financial institutions had found themselves on the end of a chaotic process, receiving numerous requests daily from FinCEN with a one-week response deadline. The requests often did not contain a clear indication of whether the information requested concerned terrorist financing or money laundering, and many in the financial sector suspected that law enforcement were submitting requests involving targets of investigations that did not relate to either.11 Financial institutions also felt that the process imposed a significant administrative burden on the private sector which in fact discouraged productive, transparent collaboration.

The private sector also argued that FinCEN’s implementing regulations were not consistent with the intent of the PATRIOT Act. Rather than encouraging a genuine exchange of information,

9. 2001 USA PATRIOT Act, Section 314 (a).
financial institutions believed that 314(a) was operating as a ‘one-way street’ in which financial institutions gathered information for the benefit of law enforcement but without receiving meaningful intelligence and information on money laundering and terrorist financing methods in return. Private sector firms were disappointed to find that law enforcement would merely provide names against which they were expected to run searches – the utility of which firms struggled to understand.\textsuperscript{12} John Byrne, then senior counsel at the American Bankers Association (ABA), testified to Congress at the time that ‘There is no better example of a positive public policy goal not being met than the implementation of section 314 of USA Patriot Act.’\textsuperscript{13}

Following a five-month pause, in February 2003 FinCEN resumed submitting Section 314(a) requests after streamlining and enhancing its processes. It began consolidating Section 314(a) requests it received from law enforcement and issuing them in bi-weekly batches; it also clarified the range of records required for searches, extended the response time to two weeks, and indicated that financial institutions are only required to respond to FinCEN where they identified positive matches.\textsuperscript{14} The two-week deadline for positive responses can be shortened or extended by the requester on a case-by-case basis.

FinCEN also clarified the scope of searches required of the private sector. Financial institutions are required to carry out a one-time search of specific record types, relating to deposit accounts; funds transfers; securities; sales of monetary instruments; trusts; commodities, options and derivatives; and safe deposit boxes. Unless otherwise specified, the scope of information which financial institutions can pass back to law enforcement through FinCEN is limited to whether the subject of interest:

- Currently maintains an account.
- Has maintained an account over the preceding twelve months.
- Has been involved in any transactions over the preceding six months.\textsuperscript{15}

Where a financial institution finds a match against its customer lists or transaction records, it is limited to responding with basic information, such as the name of the individual or entity, the numbers of any associated accounts and the date or type of associated transactions;\textsuperscript{16} only if subpoenaed for further information can the financial institution provide details of accounts or transactions. A financial institution may also use information it identifies during its searches to file an SAR on a customer or parties to a transaction.


\textsuperscript{13} Ibid., p. 4

\textsuperscript{14} Ibid., p. 5.


\textsuperscript{16} Ibid.
Another glitch in the early Section 314(a) system was that FinCEN relied on a largely paper-based and low-tech process for distributing information requests. This meant that requests often did not reach the intended financial institutions, were sent to incorrect points of contact or went unnoticed by staff at financial institutions.\textsuperscript{17} Since 2005, however, FinCEN has relied on its Secure Information Sharing System to send vetted 314(a) requests to approximately 43,000 points of contact at 22,000 US financial institutions,\textsuperscript{18} each of which must maintain a dedicated point of contact for receiving requests.

FinCEN’s reforms also involved clarifying the relevance and utility of Section 314(a) requests. After the 2002 moratorium, FinCEN began vetting law enforcement requests to ensure that irrelevant or superfluous requests were not submitted. Section 314(a) requests that law enforcement requests sent to FinCEN must now be accompanied by written attestations that the subject of the request is ‘reasonably suspected’ to be engaging in money laundering or terrorist activity, and that all other traditional means of investigation have been exhausted.\textsuperscript{19} Law enforcement must also provide minimum identifying information to allow a financial institution to locate the individual or entity in question.\textsuperscript{20}

To help financial institutions understand the value of information provided to law enforcement, FinCEN began soliciting feedback from law enforcement on the utility of requests – such as whether information financial institutions provided led to subpoenas or convictions. FinCEN publishes the results of this in its regular SAR Activity Reviews and SAR Stats reports. For example, in 2011 FinCEN published information about the value of 314(a) requests to US federal law enforcement investigations into foreign corruption.\textsuperscript{21}

**Section 314(b)**

The rationale for Section 314(b)’s drafting lies in the restrictions of the SAR process. As is the international norm, US financial institutions are generally prohibited from disclosing to one another that they have filed, or intend to file, an SAR. This presents a challenge to their attempts to compile meaningful financial intelligence on their customers; access to the SARs of other institutions, or even mere knowledge that another financial institution had filed an SAR on a customer or transaction, could assist a financial institution in conducting its own investigations. However, international standards for SARs have long held that strict confidentiality between a submitting institution and its FIU is essential to safeguarding information.\textsuperscript{22}

\textsuperscript{17} House Financial Services Subcommittee on Oversight and Investigations, ‘Testimony of John J. Byrne on Behalf of the American Bankers Association Before the House Financial Services Subcommittee on Oversight and Investigations on Progress Since 9/11’, p. 5.
\textsuperscript{19} Ibid.
Even prior to 9/11, this did not mean that financial institutions could not share any information with their peers. US regulators understood that for a financial institution to develop meaningful FININT, it must be able to share information with counterparts. FinCEN clarified in October 2000 that firms could share details about their customers or transactions that formed the basis of an SAR, so long they did not reveal the existence of an SAR.23

However, just as with public–private information sharing, post-9/11 private sector information sharing required streamlining and formalisation. From the time of the adoption of the Financial Services Modernisation Act of 1999, US financial institutions had been required to develop safeguards to protect customer data. This acted as a deterrent to widespread private–private financial information sharing, as firms feared legal action for transferring customer data. FinCEN therefore attempted to balance the requirement of banks to protect customer data with the imperative to facilitate information sharing on a broad scale. Financial institutions required a guarantee that they would not be held liable for sharing data when they did so responsibly; but if FinCEN were to offer safe harbour from liability to the private sector without strict conditions, the priority to protect customer data might fall by the wayside.

Hence, whereas private sector participation in Section 314(a) is mandatory, FinCEN’s implementing regulations made participation in Section 314(b) voluntary. Under Section 314(b), financial institutions must take several steps before sharing information: they must notify FinCEN annually of their intent to participate in Section 314(b); they must verify that any other institution with which they share information has also notified FinCEN of its intent to participate; and they must attest that they have adequate policies and procedures to safeguard the confidential information they share.24 Furthermore, information that financial institutions share may only be used for specific purposes, in particular:

- To identify, and if deemed necessary, report on money laundering or terrorist activity.
- To determine whether to open or close an account, or otherwise facilitate business.
- To assist a financial institution to carry out its AML/CTF responsibilities.25

Critically, Section 314(b) participation does not permit financial institutions to disclose to one another the fact of an SAR filing under any circumstances. If a financial institution fails to meet any of the conditions listed above, it will lose access to safe harbour.

Despite the purported benefits to their ability to collect FININT, the private sector did not react to these new authorities with unqualified cheers. Similar to its critiques of Section 314(a), the ABA voiced its concern that FinCEN’s regulations implementing Section 314(b) were too restrictive and would discourage widespread participation, for example by imposing an annual certification requirement on financial institutions. Furthermore, the ABA worried that the

25. Ibid., p. 16.
implementing regulations were not sufficiently clear about the extent of data security measures the financial sector should have in place to qualify for safe harbour.\textsuperscript{26}

The next sections will consider whether the various critiques of Section 314 are warranted.

**Fifteen Years On: Evaluating the 314 Partnership**

**Section 314’s Strengths**

FinCEN maintains that Section 314(a) ‘has proved to be successful’,\textsuperscript{27} and that Section 314(b) has ‘wrought substantial benefits for law enforcement and industry alike.’\textsuperscript{28} The comments of government and the private sector suggest that Section 314 is achieving three important objectives that were implied as part of the PATRIOT Act’s original intent.

**First, the quality of FININT available to law enforcement has improved and has assisted action against targets.** US law enforcement agencies are staunch advocates of 314(a) as a tool that makes their investigations into money laundering and terrorism more efficient. According to FinCEN, Section 314(a) ‘enables an investigator to canvas the nation’s financial institutions for potential lead information that might otherwise never be uncovered ... and allows disparate bits of information to be identified, centralized and rapidly evaluated.’\textsuperscript{29} In 2004, the 9/11 Commission noted that the Section 314(a) process ‘saves an investigator hundreds of hours that would have otherwise been spent on a bank-by-bank inquiry – an inquiry that would not have been done under the old system owing to time and resource constraints.’\textsuperscript{30}

FinCEN’s efforts to streamline the Section 314(a) process have addressed early private sector concerns that the programme would merely result in an endless stream of law enforcement requests for information. In January 2016, FinCEN publicly cited the total number of 314(a) requests filed since 2002 as 2,748, which, when extrapolated over fifteen years, does not suggest law enforcement uses the programme to make frivolous requests at the expense of financial institutions.\textsuperscript{31} At a rate of approximately 210 requests per year, use of Section 314(a) is judicious and focused. FinCEN insists that its rigorous vetting of 314(a) requests helps to ‘ensure that the 314(a) programme is utilized only in significant situations, thereby minimizing the cost to reporting financial institutions.’\textsuperscript{32}


\textsuperscript{27} FinCEN, ‘314a Fact Sheet’.


\textsuperscript{29} FinCEN, ‘314a Fact Sheet’.

\textsuperscript{30} Roth et al., ‘Monograph on Terrorist Financing’, p. 60.

\textsuperscript{31} FinCEN, ‘314a Fact Sheet’.

FinCEN’s statistics on the use of Section 314(a) also suggest that requests are successful as measured by the number of requests that lead to legal action against targets. According to FinCEN, each 314(a) request results in the identification of an average of eight accounts and sixteen transactions, and results in seven follow-up initiatives between law enforcement and financial institutions. Whilst FinCEN’s numbers do not specify the frequency of requests that may result in zero matches returned from any financial institutions among the 22,000 surveyed, it seems unlikely that many such requests exist, if at all. Indeed, law enforcement feedback to FinCEN indicates that 95 per cent of Section 314(a) requests contribute to an indictment or arrest. FinCEN notes, furthermore, that 314(a) has provided lead information related to a wide variety of criminal activity, including arms smuggling, investment fraud, cigarette smuggling, identify theft, drug trafficking and healthcare fraud.

FinCEN maintains that law enforcement agencies benefit from Section 314(b) as well. Dennis Lormel, a former counter-terrorism chief at the FBI, has written that Section 314(b) results in financial institutions producing higher quality SARs, which in turn ‘provides law enforcement with better opportunity to develop investigative evidence.’ FinCEN has publicly cited examples of cases where law enforcement investigations drew on SARs produced through financial institutions’ collaborative information exchanges under Section 314(b).

Second, participating financial institutions have had better access to information on money laundering and terrorist activity, enhancing their ability to make informed decisions about customers, accounts and transactions. Section 314(b) allows participating financial institutions to have more than a siloed view of activities that occur in-house; rather, the ability to share information with other financial institutions can provide a financial institution with a holistic, end-to-end view of customer activity. As Lormel explains:

> When financial institutions participate in Section 314(b) information sharing, they have an opportunity to obtain information regarding customers who pose concerns to them. It enables them to go back in the direction of the source of funds and get closer to the origin, and to go forward to the use and get closer to the point of distribution. This information, which is provided by other participating financial institutions, can assist in making decisions to file SARs. It will also provide better details to include in SAR narratives.

In addition to obtaining better quality information that they may use to file an SAR, financial institutions may also use Section 314(b) to inform their decisions about customers. For example, an institution that receives information from a peer can use that information to make decisions about whether to continue or terminate a customer relationship. Furthermore, if a financial

---

33. FinCEN, ‘314a Fact Sheet’.
34. Ibid.
35. Ibid.
38. Lormel, ‘Section 314(b) Information Sharing Revisited’.
institution has information on a customer that appears suspicious at first glance, it may obtain information from its peers which clarifies that an SAR is not warranted. This can save both the private and public sector valuable time and resources that might be lost processing SARs of limited intelligence value.

It is not only Section 314(b) that benefits the private sector. Historical claims that Section 314(a) is a ‘one-way street’ benefiting law enforcement at the expense of financial institutions seem oversimplified. Once early procedural glitches were fixed, financial institutions have generally viewed processing Section 314(a) requests as a largely uncontroversial compliance procedure, even if the process of searching multiple internal customer databases for matches can prove challenging.

More pointedly, however, Sections 314(a) and (b) are part of a broader, iterative process of information sharing that benefits financial institutions: US regulators have clarified that financial institutions can share information under Section 314(b) with their eligible peers using information they uncover whilst conducting investigations into 314(a) subjects on behalf of law enforcement. Similarly, financial institutions may make decisions about whether to retain or terminate a customer relationship based on information uncovered whilst responding to a 314(a) request. Section 314(a) requests also provide financial institutions with concrete, albeit limited, information about specific security threats of concern to law enforcement. Sharing any additional information beyond the names of subjects with such a broad swath of the US financial sector is likely impractical; law enforcement has the legitimate concern that sharing details of investigations could jeopardise them. Whilst it may not function as a truly ‘two-way street’, now that its early inefficiencies have been addressed, Section 314(a) could be fairly described as a highly valuable ‘one-and-a-half-way street’.

Third, a culture of responsible, secure information sharing has emerged among participating financial institutions. Since 9/11, the US public and private sectors have developed a better understanding of one another’s roles in fighting financial crime, as well as the respective challenges they face. Whilst improved interaction between the private and public sectors is the result of numerous factors, experts consulted during the preparation of this study cited Section 314 as playing a direct and important role in the US context.

Financial institutions function both as the gatekeepers of secure customer data and as the first line of defence against financial crime. They must, therefore, walk a delicate line when it comes to information sharing. Section 314(b) embodies a culture of information sharing that is responsible, thorough and transparent. Whether this has extended to the US financial system on a large scale is debatable. However, FinCEN points to two factors that it believes indicate Section 314(b) practices are expanding across the US private sector.

41. Lormel, ‘Section 314(b) Information Sharing Revisited’.
42. Author’s discussions with experts, February 2016.
First, the number of SARs US financial institutions have filed under Section 314(b) has grown steadily since 2002. FinCEN encourages financial institutions to reference Section 314(b) when filing SARs based on information shared under it. In 2004, FinCEN received approximately 500 such SARs; in 2012, it received over 3,500. This seven-fold increase suggests that knowledge and awareness of the programme and its benefits is growing among US financial institutions.

Second, more non-bank financial institutions are participating in Section 314(b). FinCEN has noted, for example, that securities firms and broker-dealers have steadily filed a growing number of Section 314(b) SARs both in absolute numbers, and as a percentage of all Section 314(b) SARs. Additionally, FinCEN notes that various types of financial institutions are able to share information together under Section 314(b). As FinCEN puts it, ‘the synergy developed between 314(b) participants from different sectors of the financial system – for example, between an online broker-dealer and a bank – creates opportunities for cross industry sector information sharing’.

The fact that Section 314(b) participation is available to a broad range of US financial institutions offers the potential for flexibility and dynamism in the US private–private information-sharing programme. After all, criminals and terrorists rely on the US financial sector as a whole, not only a segment of it. The ability to facilitate sector-wide information sharing is essential if the programme is to succeed in providing comprehensive, actionable information on threats.

**Reasons for Success**

Several characteristics of the US information-sharing approach, as implemented through Section 314, underlie these successes.

**The Section 314 process has been genuinely collaborative and has shown trust in the private sector.** Under Section 314(a), a large number of financial institutions are entrusted to handle sensitive law enforcement information. With 314(b), the private sector is entrusted to proactively identify threats. This promotes the notion that financial institutions are a critical partner for law enforcement and not merely a tool. Furthermore, the process is iterative: participating institutions receive information on subjects from law enforcement, which in turn may lead to SARs, which can in turn lead to further law enforcement follow-up with the private sector. A sense of genuine partnership is essential to maintain the private sector’s motivation and productive participation.

44. FinCEN’s guidance indicates that all financial institutions, or an association of financial institutions, subject to AML regulations, are eligible to participate in Section 314(b), this includes: banks, casinos and card clubs; money service businesses; brokers or dealers in securities; mutual funds; insurance companies; futures commission merchants and introducing brokers; dealers in precious metals, precious stones, or jewels; operators of credit card systems; and loan or finance companies.
The US approach has been dynamic. Since it began implementing Section 314, the US government has demonstrated a willingness to adapt to meet the needs of its users. As already discussed, FinCEN was quick to respond to the concerns of the private sector in the early phases of Section 314(a) implementation. This responsiveness has helped the private sector to accept the programme and understand its benefits.

In light of the positive feedback it received over the years from US federal law enforcement agencies, FinCEN has also taken steps to expand the benefits of Section 314(a) to other law enforcement bodies. In 2010, FinCEN amended its regulations to extend the ability to make Section 314(a) requests to the following range of agencies: foreign law enforcement agencies subject to the US–EU agreement on mutual legal assistance; US state and local law enforcement agencies; and FinCEN itself, which had previously only been allowed to facilitate Section 314(a) requests, but under the 2010 amendments was given authority to initiate them independently.47 To ensure that this expanded law enforcement access to Section 314(a) does not result in a return to an excessive number of requests being submitted to the private sector, FinCEN will need to continue operating a robust system for vetting requests and to solicit feedback about the impact of the expanded programme on the private sector’s compliance efforts.

Section 314 has been complemented by other measures (including Section 311) that alert the private sector to specific financial crime risks. Section 314 information sharing does not occur in a vacuum. Other provisions of US law offer means by which the public and private sectors can share information on specific threats. The second part of this paper will examine the most significant of these: Section 311 of the PATRIOT Act. But first it is worth mentioning another of the tools available to FinCEN: geographic Targeting Orders (gTOs). Under the US Bank Secrecy Act, the director of FinCEN may issue gTOs to temporarily require enhanced record-keeping and reporting requirements of certain regulated business in a specified geographic area. For example, in January 2016, the director of FinCEN issued a gTO requiring certain title insurance companies to report the identity of beneficial owners of shell corporations used to purchase residential properties in Manhattan and Miami.48 FinCEN cited the significant money laundering risks associated with shell corporation purchases of property in these locations as warranting ‘a risk-based approach to combating money laundering in the real estate sector.’

GTOs allow FinCEN to compel the private sector to conduct intelligence gathering in relation to a specific risk and, in turn, provide US financial institutions with information about high-risk activities that FinCEN sees as high priority. Taken alongside the broad-based information-sharing provisions of Section 314, GTOs offer an additional method to facilitate public–private exchanges utilising a risk-based approach.

47. ‘Financial Crimes Enforcement Network; Expansion of Special Information Sharing Procedures To Deter Money Laundering and Terrorist Activity’, Federal Register, Vol. 75, No. 27, 10 February 2010, pp. 6,560–70.
The Limitations of Section 314

Even if it seems fair to conclude that Section 314 has established an important basis on which the US can expand private–public information-sharing partnerships, US policy-makers nevertheless admit that Section 314 has not achieved the success that they hoped for, and that further enhancements are necessary.

This is especially true of Section 314(b). In 2012, Stuart Levey, the former US Treasury under-secretary for terrorism and financial intelligence, commented in Congressional testimony that Section 314(b) ‘has not been used as robustly as it might be.’

For example, as noted earlier, in 2012 US financial institutions filed more than 3,500 SARs that made reference to information sharing under the Section 314(b) programme. That same year – the last for which the numbers of Section 314(b) SARs are publicly available – US financial institutions filed over 1.5 million SARs. FinCEN acknowledges that the number of SARs filed with specific reference to Section 314(b) in their narratives is not necessarily indicative of the total number of SARs that may have been filed whilst drawing on Section 314(b) information sharing (there may be countless instances where the submitting institutions failed to reference the programme). While absolute numbers do not negate the claim that Section 314(b) SARs are of significant intelligence value to law enforcement, it is still the case that ten years after the passage of the PATRIOT Act, SARs referencing Section 314(b) formed only 0.002 per cent of all SARs filed with FinCEN. This casts doubt on the claim that the US financial sector as a whole is aware of and uses Section 314(b) provisions.

Similarly, whilst FinCEN publicly touts growing participation in the Section 314(b) programme by a range of non-bank financial institutions, there is reason to be sceptical that the US financial sector as a whole has reaped the full benefits of Section 314(b). Experts consulted during the drafting of this report noted that banks are generally reluctant to share information with non-bank financial institutions, such as money service businesses, jewellery dealers and casinos. This may be because of general inexperience in cross-sector collaboration among many Section 314(b) participants, as well as doubts among large banks that they can trust smaller, non-bank institutions to keep information secure.

FinCEN has undertaken a sustained public outreach campaign to increase the participation of non-bank financial institutions in Section 314(b). In 2014, FinCEN indicated that nearly 100 gambling institutions had joined the Section 314(b) programme. This certainly marks a step forward, and suggests that FinCEN’s sector-focused outreach campaigns can have an impact.

51. Author’s discussions with experts, February 2016.
But the fact that it has taken nearly a decade and a half to obtain non-bank financial institution participation of consequence suggests US regulators are playing catch-up. Furthermore, hurdles remain to cross-sector engagement. In 2015 the director of FinCEN, Jennifer Shasky Calvery, publicly noted that ‘despite the [safe harbour] protections offered, some banks are not responsive to requests from casinos to share information.’\(^5\)

The de facto exclusion of the non-bank financial sector from information-sharing arrangements extends to Section 314(a) as well. Whilst all financial institutions subject to AML/CTF regulations in the US must have in place a programme to receive and comply with Section 314(a) requests, the requests do not, in fact, reach the broad range of US financial institutions covered by AML/CTF legislation. As one observer notes, because Section 314(a) regulations require financial institutions to search their records for accounts and transactions, ‘account’ and ‘transaction’ are specifically defined in relation to banks: ‘an “account” is defined as a formal banking or business relationship … Similarly, a “transaction” refers to activity most commonly associated with banks, credit unions, and securities and commodity broker dealers.’\(^5\) As a result, these institutions receive the bulk of FinCEN’s automated 314(a) requests.\(^5\) FinCEN has acknowledged that many non-bank financial institutions covered by AML/CTF legislation have been excluded from 314(a) requests, but has indicated its intention to extend Section 314(a) requests to the broader spectrum of the regulated financial sector.\(^6\)

Even among the mainstream banking sector, some experts note that the frequency of information sharing under Section 314(b) has failed to meet expectations and that where participation has occurred, it has not been as robust or frequent as had been intended at the outset of the PATRIOT Act.\(^7\) One common reason cited for the hesitancy to participate is that banks are reluctant to share sensitive commercial information with their competitors. Another is general anxiety about data privacy protections. Even with very strong safe-harbour provisions in place, some private sector actors will inevitably be reluctant to share sensitive customer information in certain cases, particularly where they receive requests to share information from financial institutions they have not collaborated with previously. Whilst commercial and legal concerns are certainly likely to impact decisions about information sharing, three aspects of Section 314 implementation may have hindered information-sharing efforts to date.

First, the public and private sectors have struggled to achieve consensus around the scope and intent of key provisions in Section 314. Since the inception of Section 314(b), financial

---

55. Ibid.
57. Author’s discussions with experts, February 2016.
institutions have expressed confusion over the extent of information they can share whilst retaining safe harbour. One concern the private sector commonly cites concerns the wording of the statute that information shared must relate to ‘terrorist or money laundering activities’. Some in the financial sector have indicated that this language is not sufficiently broad to give them the comfort they need to share information related to fraud and certain other predicate offences to money laundering.58

In response to these views, in 2009 FinCEN issued guidance clarifying that under 314(b) a financial institution ‘may share information relating to transactions that the institution suspects may involve the proceeds of one or more [predicate offences to money laundering] … [which] include an array of fraudulent and other criminal activities.’59 FinCEN’s outreach campaigns to the private sector have included emphasising its view that the language of Section 314(b) is sufficiently broad to allow information sharing on a wide range of activities. FinCEN has also cited examples of SARs filed under Section 314(b) involving money laundering related to a wide range of underlying crimes, including market manipulation, counterfeiting, insurance fraud, cheque fraud and mortgage fraud.60 This indicates that at least some private sector participants use Section 314(b) for broad purposes. However, FinCEN has publicly acknowledged that some financial institutions remain confused about the types of criminal activity on which they may share information.61 This suggests that some in the private sector struggle to understand both the literal text of the legislation and its implementing regulation, as well as its overarching objectives.

Most observers generally regard Section 314(a) as the more successful of Section 314’s provisions. Section 314(a) also offers lessons about legislative clarity and intent. The drafters of the law envisaged a genuine exchange of information between the public and private sectors. When the public sector drafted implementing regulations, it took a narrow, literal view of the intent of Section 314(a). The private sector, however, had expectations that Section 314(a) would facilitate a freer exchange of more detailed information from law enforcement. The lack of consensus among stakeholders about the law’s intent resulted in significant early glitches in the implementation of Section 314(a) that might otherwise have been avoided.

Part of this confusion may be attributable to insufficient clarity in the language of Section 314 and its implementing regulations. More broadly, however, it speaks to the importance

58. ‘Predicate offenses’ refer to the types of underlying criminal activity that can lead to a money laundering offence. For example, drug dealing is a stand-alone criminal offence; where drug dealing generates funds, drug dealing acts as the predicate offence to money laundering. The UK has an ‘all crimes regime’, in which money laundering can be linked to all types of underlying offences. The US, on the other hand, links money laundering offences to certain ‘specified unlawful activities,’ or specific crimes which can lead to a separate money laundering offence.
of achieving consensus among the public and private sectors over the ultimate objectives of information-sharing arrangements prior to undertaking their widespread implementation.

**Second, Section 314 has not been supported by robust technical platforms and mechanisms to facilitate practical information sharing.** Despite providing a legal basis, the enactment of Section 314 did not solve the problem of how to share information. Widespread implementation took place before suitable technological arrangements were in place and before processes had been tested on a small scale. Today, FinCEN uses a centralised electronic platform for distributing information requests to law enforcement under 314(a). This system, however, was not implemented until three years after adoption of the implementing regulations. In the early years of Section 314(a)’s implementation, the lack of a functioning and tested platform for sharing information meant law enforcement requests were often not distributed or processed properly; similarly, many financial institutions at the time lacked automated systems for conducting searches across multiple customer databases so had to search names manually, adding significantly to their compliance burden.62 Today, a variety of automated compliance solutions exist to assist the private sector in conducting Section 314(a) searches.

Whilst now resolved in the case of 314(a), a resource-intensive, cumbersome process for exchanging information continues to hinder Section 314(b) participation. The practicality of sharing information with peers remains problematic for many US financial institutions, even fifteen years after Section 314(b)’s adoption. If a financial institution wishes to share information under 314(b), it faces numerous challenges. Among these are fundamental difficulties of networking and communication. At present, FinCEN provides Section 314(b) participants with a list of all other financial institutions that are registered under the programme. However, if a financial institution has concerns about a particular individual or entity, merely knowing the identities of other Section 314(b) participants does not tell them which other financial institutions may possess information relevant to those concerns. One observer likens the process of identifying institutions that have information about a particular individual or entity to ‘looking for a needle in a haystack … except you don’t know which haystacks to look in.’63 Section 314(b) participation can therefore be time-consuming and inefficient.

Fortunately, technology is changing the picture. Financial institutions and IT firms have begun to develop a number of solutions to facilitate Section 314(b) exchanges. The use and development of these products is still not widespread, but they may offer the potential for future increases in participation. These platforms attempt to streamline the process of interacting with other programme participants, whilst allowing each participant to maintain control of its data. These solutions provide a centralised exchange on which registered Section 314(b) participants can make enquiries within a network of peers to determine whether other institutions maintain information on a particular individual or entity. The systems keep customer data anonymous, employing algorithms to provide a score indicating the likelihood of a match with another participating institution, and offer guidance as to whether the information meets the legal

---

requirements for sharing under Section 314(b). Where a match is found, financial institutions may then communicate with one another to arrange for sharing information. The aim of these products is to provide a streamlined mechanism for Section 314(b) networking, the lack of which has likely set participation back a number of years.

Some former US government officials have also noted that, for all the benefits of Section 314, its platforms do not facilitate information sharing quickly enough to keep pace with real-time threats. They advise that Sections 314(a) and (b) should be supplemented by co-operative fora in which financial institutions can discuss and share real-time information on threats with the public sector. For example, as early as 2007, a former US Treasury official, Robert Werner, noted that to help Section 314(a) function as a genuinely ‘two-way street’, ‘Working groups composed of government and private sector officials should be developed and modeled on relationships between the Defense Department and its contractors. If appropriate, officials at financial institutions should receive security clearances to constructively participate in these discussions.’

The practicality of allowing the federal government to share classified information with financial institutions is a complex one – one that the 9/11 Commission advised against in its 2004 monograph on terrorist financing, for fear that the risk of jeopardising classified information outweighed the benefits. Werner’s point nevertheless highlights a general conundrum: even though law enforcement receives actionable information under Section 314(a), and financial institutions may file better quality SARs using information shared under Section 314(b), the Section 314 processes may not always be rapid enough, or closely co-ordinated enough, to target criminals’ or terrorists’ financial activity during time-sensitive, complex investigations.

To this end, FinCEN has recognised the need to evolve into a more proactive entity, increasing its data-analytic capabilities and working not only to facilitate, but to promote and initiate, information exchanges. In 2014, Director Calvery acknowledged that the private sector has expressed the view that FinCEN should promote ‘more dynamic, real-time information sharing, both by and between financial institutions, and with FinCEN and law enforcement.’ FinCEN has indicated that it is working on pilot programmes to facilitate improved Section 314 information sharing, and has established an Intelligence Division, which has responsibility for expanding FinCEN’s provision of analytical products to the private sector.

Third, in its implementation of Section 314, the US is still adapting to a contemporary view of financial crime and related compliance challenges. It should come as no surprise that implementation of a law enacted in 2001 has at times been slow to adapt to the rapidly evolving

---

67. Ibid.
nature of international finance and accompanying crime. Whilst the US government has taken a number of important steps to update the Section 314 regime, there are a number of respects in which implementation could benefit from continued adaptation and modernisation.

For example, Section 314 treats money laundering and terrorist financing as problems separate from the range of other compliance challenges financial institutions face. In 2012, a collection of financial institutions indicated their intent to share data on fraud activity over IT platforms similar to those described above. FinCEN clarified that when sharing information on fraud offences under 314(b), financial institutions may only count on safe harbour where the fraud involves a transaction that is suspected to have generated criminal proceeds; sharing information about fraudulent activity that has not resulted in transactions that constitute money laundering, such as a customer falsifying information on a loan application but where the loan was not disbursed, would appear not to be permitted under Section 314(b).

Financial institutions have expressed the view that distinguishing activities such as fraud from money laundering poses a practical challenge. Furthermore, given that many financial institutions are increasingly integrating AML/CTF, fraud and other financial-crime functions within their compliance departments, an approach that treats the risks of money laundering and its predicate offences as clearly segregated problems may be outdated.

Another limitation of Section 314 is that it is US-centric. As noted earlier, FinCEN has extended 314(a) participation to certain foreign law enforcement agencies. Section 314(b), however, still applies only to information shared between US financial institutions. Sharing information under 314(b) with foreign financial institutions is strictly prohibited – including a US financial institution sharing information with its foreign branches or subsidiaries. This hinders the ability of US financial institutions to develop FININT about customers in an increasingly globalised financial system. The practical and legal challenges involved in expanding information sharing internationally are beyond the scope of this paper, but it is nonetheless worth noting this existing limitation to 314(b).

II. Section 311: Special Measures, Primary Concerns

In Section 311 – ‘Special Measures for Jurisdictions, Financial Institutions, or International Transactions of Primary Money Laundering Concern’ – the PATRIOT Act provides FinCEN with powers that compensate for some of the challenges of Section 314 implementation. Where the secretary of the Treasury determines that a foreign jurisdiction, financial institution, class of transaction, or type of account represents a ‘primary money laundering concern’, financial institutions are compelled to place the target under increased scrutiny and restrict access. Where FinCEN has at times found itself frustrated by the reluctance of many financial institutions to share information under Section 314(b), Section 311 offers FinCEN a tool for mandating that the whole of the US financial system engage in carefully tailored FININT collection techniques on specific targets.

In doing so, Section 311 aims to ensure that the private sector is informed about specific priority threats, that the public sector receives quality FININT on those threats, and that the public sector is able to employ that information to disrupt threats.

Laying a Foundation: The Origins and Intentions of Section 311

As in the case of Section 314, the impetus for Section 311 authorities was the deficiency of the US’s AML/CTF regime that policy-makers had recognised even before 9/11.

Consequently, by the summer of 2000, Congress had begun to consider legislation that would enhance the ability of the Treasury to protect the domestic and international financial systems from severe threats. In July of that year, Senator John Kerry introduced to the Senate a bill, the International Counter-Money Laundering and Foreign Anticorruption Act,71 to permit the secretary of the Treasury to designate a foreign financial institution as a concern and invoke a range of measures to mitigate those threats.72 The intent of these proposed measures was twofold: first, to keep tainted foreign financial institutions that facilitated financial crime out of the US financial system; and second, to encourage any jurisdictions where such institutions operated to strengthen their AML laws in line with FATF standards.73

Whilst Senator Kerry’s proposed measures failed to achieve Congressional support in 2000, 9/11 saw them revived and expanded in Section 311 of the PATRIOT Act. Specifically, Section

72. Tracey, ‘Using the Patriot Act to Turn North Korea’s Dirty Money into a Bargaining Chip’, p. 130.
73. Ibid.
311 authorises the secretary of the Treasury to determine that a foreign jurisdiction, financial institution, class of transaction or type of account represents a ‘primary money laundering concern’. This authority is delegated through regulation to the director of FinCEN. Upon making a determination that a foreign target merits the classification of a primary money laundering concern, the director of FinCEN may invoke the following special measures, alone or in combination, which impose requirements for US financial institutions related to:

1. Record-keeping and reporting of certain financial transactions.
2. Information relating to beneficial ownership.
3. Information relating to certain payable-through accounts.
4. Information relating to certain correspondent accounts.
5. Prohibitions or conditions on opening or maintaining certain correspondent or payable-through accounts.

Section 311 provides FinCEN with enormous latitude in determining the types of financial institutions and jurisdictions to target, allowing for flexibility in addressing a broad array of threats. The statute sets out factors that FinCEN may consider when determining if a foreign financial institution is a primary money laundering concern, including whether:

- The financial institution facilitates money laundering.
- The financial institution has any legitimate functions.
- Taking action against the financial institution is likely to assist in protecting the international financial system from financial crime.\(^{74}\)

Similarly, when considering Section 311 action against a jurisdiction as a whole, FinCEN has leeway to consider a broad range of factors, including whether:

- There is evidence that organised criminals or terrorists do business in the jurisdiction.
- The jurisdiction offers bank secrecy to non-residents.
- The jurisdiction has strong bank supervision and AML laws.
- Credible international organisations regard the jurisdiction as an off-shore secrecy haven.
- The jurisdiction has high levels of corruption.\(^{75}\)

To date, FinCEN has found nineteen foreign financial institutions and four foreign jurisdictions as being of primary money laundering concern. Among these are:

- Liberty Reserve, a Costa Rican virtual currency exchange that facilitated activity by money launderers, fraudsters, cyber-criminals and a range of other illicit actors.
- Banco Delta Asia, a financial institution in Macao that facilitated illicit financial activity on behalf of the North Korean regime.
- The Commercial Bank of Syria, for facilitating widespread money laundering activity, and in light of Syria’s overall AML/CTF deficiencies.

\(^{74}\) 2001 USA PATRIOT Act, Section 311, para. 3(c)2(B).
\(^{75}\) Ibid., Section 311, para. 3(c)2(A).
- Lebanese Canadian Bank, a Beirut-based financial institution that international drug traffickers and the terrorist organisation Hizbullah used to launder funds.
- Banca Privada d'Andorra, an Andorran bank with an international presence, whose senior management facilitated activity on behalf of organised criminals, human traffickers and fraudsters.
- The Islamic Republic of Iran, which has been the subject of FATF calls for countermeasures in light of overall AML/CTF deficiencies in its financial system, and whose financial institutions have facilitated proliferation and terrorist activity.\(^76\)

### Section 311 Successes

FinCEN’s implementation of Section 311 has facilitated three broad aims of the PATRIOT Act.

**First, Section 311 has allowed the US government to alert financial institutions to a diverse range of high-priority threats.** When it identifies a foreign jurisdiction or financial institution\(^77\) as being of primary money laundering concern, FinCEN provides the US financial sector with important concrete information about the nature of financial-crime threats. The Treasury publishes detailed notices and findings that make available unclassified (or declassified) information on the target institution or jurisdiction, outlining the reasons FinCEN has deemed it a primary money laundering concern. These notices provide financial institutions with critical details about a target’s illicit financial activity and equip them to monitor and guard against those threats. In this respect, Section 311 counterbalances the private sector’s perceptions of Section 314 that they are on the giving end of a ‘one-way street’ when it comes to information sharing.

**Second, FinCEN has drawn on its Section 311 authority to single out threats for targeted FININT collection.** Of the five special measures Section 311 offers FinCEN, four involve requirements that US financial institutions generate information on the financial activity or ownership of the target financial institution or jurisdiction. For example, in April 2013, FinCEN issued findings on Halawi Exchange and Rmeiti Exchange, two Lebanese exchange houses that facilitated money laundering on behalf of Hizbullah. FinCEN proposed to invoke the first special measure in relation to both entities, which would require US financial institutions to file reports to FinCEN of any transactions, or attempted transactions, related to the two exchange houses.\(^78\)

On issuing its notice of proposed rule-making, FinCEN noted that these reporting requirements would:

76. Information on these and other Section 311 actions can be found at <https://www.fincen.gov/statutes_regs/patriot/section311.html>.
77. Whilst Section 311 provides the authority to label a class of foreign transaction or type of account as posing a primary money laundering concern, so far FinCEN has only directed its Section 311 actions at foreign jurisdictions and financial institutions.
help FinCEN and law enforcement identify other participants in the money laundering schemes ... which would be utilized in efforts to detect and deter these and other financial crimes. Such efforts would enhance national security by making it more difficult for terrorists and money launderers to access the substantial resources of the U.S. financial system.79

FinCEN had previously proposed the same measure in the case of JSC CredexBank, a Belarusian bank that facilitated money laundering on behalf of shell corporations. FinCEN’s proposed rule on the matter indicated that, within ten days of identifying a transaction involving JSC CredexBank, US financial institutions were required to report details including the value and purpose of the transaction, the number of any identified related accounts and the identity of persons involved in the transaction. FinCEN justified its proposed imposition of the first special measure by noting that:

information gathered through reports submitted by financial institutions ... will provide FinCEN and law enforcement with greater insight into transactions or attempted transactions related to Credex, including details regarding the underlying beneficial owners. This knowledge, in turn, could help FinCEN and law enforcement pierce the veil of the shell corporations behind which the true owners of the funds involved hide.80

In its proposals to invoke this special measure, FinCEN has indicated that private sector reporting should be made directly to FinCEN outside the traditional SAR process, expediting the receipt of information about the target. The rationale behind this measure is straightforward: some threats to the financial system are too significant to be left to the traditional SAR process.

Section 311 therefore allows the US public sector to inform the private sector of a specific financial-crime threat; to compel specific reporting requirements related to that threat; and to direct the attention of the US financial system as a whole toward isolating that target for further regulatory or law enforcement action.

Third, Section 311 has allowed FinCEN to disrupt target activity in support of US and international security aims. Under the fifth special measure, FinCEN can prohibit or limit US financial institutions from opening or maintaining correspondent accounts or payable-through accounts for the target of primary money laundering concern, or on behalf of any of its subsidiaries, branches or other components. The measure has the effect of cutting off or limiting target access to US dollar clearing facilities. This way, FinCEN can shut the target out of the US financial system. Furthermore, the fifth special measure can often result in the target being denied access to the global financial system: non-US financial institutions frequently refuse to do business with the target at the time of FinCEN’s proposed findings for fear of suffering damage to their own business relationships with the US.

For example, in the case of FBME Bank, one of its European correspondents, Commerzbank, indicated that it would terminate its relationship with FBME, including closing FBME’s US dollar and non-US dollar accounts, upon FinCEN’s implementation of a final rule invoking special measure five against FBME.81

Furthermore, FinCEN’s findings have prompted foreign regulators to take action against targeted institutions. In the case of Lebanese Canadian Bank, following FinCEN’s proposal to invoke special measure five, Lebanon’s regulators moved to revoke its banking licence, and the bank’s assets were completely liquidated.82 Similarly, after the finding against Banca Privada d’Andorra, Andorran regulators moved to suspend the authority of the bank’s board, arrested its chief executive officer and sold off most of its assets to other banks.83

Significantly, in both the Banca Privada d’Andorra and Lebanese Canadian Bank cases, the mere threat of invoking special measure five led non-US regulators to take extraordinary measures against the target institutions; FinCEN had only publicly proposed a notice of intent to invoke special measure five, but withdrew the action because of the Andorran and Lebanese regulators’ swift response.

Advantages of the Section 311 Approach

Several features of FinCEN’s Section 311 implementation have enabled the achievements outlined above.

The Section 311 process has been collaborative and mutually beneficial, drawing on the capabilities of, and providing benefits to, both the public and private sectors. FinCEN relies on traditional SAR filings and other standard confidential reporting from US financial institutions to determine that a particular target is a primary money laundering concern.84 For example, FinCEN’s July 2014 finding on FBME Bank describes in detail the nature and scope of FBME’s illicit activity through the US financial system, which entailed hundreds of millions of dollars’ worth of suspected money laundering activity. The finding also cites an instance of a US financial institution having closed its account with FBME.85 Whilst the finding does not make reference

82. ‘Withdrawal of the Proposed Rulemaking against Lebanese Canadian Bank,’ Federal Register, Vol. 80, Issue 194, pp. 60,575–76.
to specific SAR filings, the disclosure of which is impermissible under US law, its descriptions of activity were drawn from FinCEN’s collective analysis of numerous individual SAR filings from US financial institutions. The process, therefore, is one in which financial institutions provide limited, fragmented information to FinCEN, which in turn consolidates that information to provide the private sector with a fuller picture of a significant and serious threat.

By publishing these findings in a publicly available document – though without reference to the specific source of information – FinCEN can signal to the private sector that the information it receives from financial institutions is of significant value. These findings in turn give financial institutions a clear indication of specific threats to which they should direct their resources and reporting efforts. This underscores, furthermore, that Section 311 is more than a one-way street through which the public sector imposes a burden on financial institutions, but rather is part of a more complex process in which shared information and feedback can lead to meaningful action.

**Section 311 has enabled FinCEN to proactively direct intelligence-gathering.** By invoking Section 311’s information-gathering measures, FinCEN becomes more than a passive recipient of SAR data from financial institutions. Section 311 promotes the notion that an FIU, as the focal point for all of a country’s FININT, should take a proactive role in driving the direction of intelligence gathering throughout the financial system. Rather than relying exclusively on the traditional SAR regime to generate a broad range of FININT, Section 311 allows FinCEN to employ its analytical capabilities to identify specific threats to the US financial system and to direct the private sector’s use of FININT-gathering capabilities in a risk-based manner.

**Section 311 has relied on a rigorous process which has promoted discretion in its use.** FinCEN does not have unlimited authority to make a finding that an entity or jurisdiction is a primary money laundering concern and thus to impose special measures. When determining which special measures to invoke, FinCEN oversees the process, but is required to consult with, and receive commentary from, the Department of State and other federal agencies prior to issuing its formal findings. The Section 311 process therefore contains a number of checks and balances. Furthermore, the PATRIOT Act requires that the Treasury take certain factors into account before making a Section 311 finding, such as whether the action would create a compliance burden for US financial institutions; would disrupt the international payments system; and is consistent with US foreign policy goals.

Some private sector representatives argue that Section 311’s special measures can create an unreasonable administrative burden. With special measures one to four, some financial institutions express the view that the paperwork and expedited reporting requirements involved pose a significant compliance challenge. Similarly, with special measure five, some in the private sector indicate that limiting the access of Section 311 targets to correspondent

banking facilities is not as simple as it sounds; in practice, it is a complex endeavour that puts US financial institutions at risk of non-compliance in the absence of additional information from FinCEN about the full range of associated parties who might act for, or on behalf of, the target.\(^8\)

In response to these views, FinCEN maintains that it weighs the potential impact on US financial institutions carefully before issuing Section 311 decisions. Indeed, the text of Section 311 obligates FinCEN to take into account the compliance burden on US financial institutions before deciding to invoke any special measures. FinCEN points out, furthermore, that many compliance solutions—such as automated screening systems—which financial institutions rely on to comply with their general AML requirements are generally easy to direct at the activity of Section 311 targets. In truth, both FinCEN and the private sector make legitimate points: successful private sector implementation of Section 311 requires clearer guidance from FinCEN, whilst the private sector bears some responsibility for adapting and innovating solutions that ensure they are able to fulfil policy objectives. As is the case with Section 314, ongoing collaboration and consensus building among the public and private sectors is critical if these measures are to remain current and impactful.

It is also worth noting that the length of time any particular special measure applies is generally limited. Measures FinCEN invokes under Section 311 are only effective for 120 days, unless FinCEN extends them through a further ruling. As mentioned, in a number of cases FinCEN’s proposed special measures have not formally gone into effect; the mere threat of their imposition proves sufficient to compel changes in behaviour. With respect to those special measures that do take effect, even if financial institutions have a valid point that they result in a compliance burden, this burden is ultimately mitigated by the fact that the measures are often revoked when the target in question has gone out of business.

Disadvantages of the Section 311 Approach

Despite the advantages Section 311 offers FinCEN in FININT-gathering and targeting threats, two features of Section 311’s use are worthy of consideration should other jurisdictions wish to empower their public sector bodies with similar tools.

The impact of Section 311 has rested heavily on the reach of the US financial system. Some observers argue that the success of Section 311 in disrupting target activity owes less to the precise design of its measures than to the US aggressively exploiting its clout in the international financial system to blacklist targets.\(^9\) Whether or not this assessment is fair, most other jurisdictions are unlikely to have as powerful an impact on targets unilaterally. Whilst countries might wish to create powers like Section 311 to guard their domestic financial systems against

---


targets and to improve FININT collection capabilities, attempting to use those same powers to compel broad changes in behaviour may not be a realistic goal.

Section 311 has placed significant authority in the hands of a single government body in a manner that might not have been possible outside the context of the 9/11 attacks. Whilst the US government had explored the potential for Section 311-type authority prior to 9/11, it was only after the attacks that it enacted Section 311. Without the impetus of the attacks, it is unclear whether FinCEN would have had the great latitude and scope to target specific threats in the manner it does now. The concentration of these authorities in FinCEN’s hands has not been without controversy; The Economist, for example, recently questioned the legitimacy of the Section 311 process, and two financial institutions that have been targeted have launched legal challenges to the findings FinCEN has made against them, claiming that the process is opaque and arbitrary.\textsuperscript{90} Other countries would undoubtedly have to give careful consideration to giving their FIUs or other governmental bodies such sweeping powers.

\textsuperscript{90.} Ibid.
Conclusion and Recommendations

INTERNATIONAL POLICY-MAKERS AGREE that more robust public–private information-sharing partnerships are necessary to bolster AML/CTF efforts. Making FININT collaboration work, however, is an enormous challenge.

Determining the scope of legal powers, developing technological platforms for sharing information, and safeguarding sensitive data are among a host of challenges policy-makers face when attempting to build public–private partnerships. As they confront this task, policy-makers should carefully consider the US experience in implementing Sections 314 and 311 of the PATRIOT Act.

The public–private information-sharing provisions of Sections 314(a) and (b) of the Act have improved the quality of FININT available to US law enforcement and financial institutions; enhanced the public sector’s ability to pursue legal action against targets; and have cultivated a culture of responsible information sharing among participants. However, private sector participation in Section 314(b) has been limited by insufficient platforms for facilitating information sharing; furthermore, the perception within financial institutions that there is a lack of clarity around fundamental provisions of the law has also discouraged participation.

US officials are aware of these limitations in Section 314 and are working to correct them. Ongoing technological innovations, attempts to clarify the intent of the law, and FinCEN’s transition to a more proactive, data-driven FIU offer hope that Section 314 implementation will keep pace with evolving threat environments.

The special measures of Section 311 have proved an important tool for singling out perceived threats to the US financial system, and have offered a focused complement to the broad information-sharing provisions of Section 314. Section 311 offers FinCEN the ability to direct US financial institutions to undertake risk-based intelligence gathering on high-priority threats. In doing so, it prompts focused and rapid FININT generation that bypasses the traditional SAR process.

FinCEN’s decisions to employ special measures under Section 311 can have a significant disruptive impact; however, this impact rests in large part on the reach of the US throughout the global financial system and it is not at all certain that other jurisdictions could have such a significant effect without co-ordinated multilateral action.

The US experience in public–private information sharing offers important lessons about the need to think carefully through the challenge of information sharing. When seeking to develop FININT collaboration programmes, policy-makers should consider the following principles,
which can assist them in harnessing the strengths of the US approach whilst avoiding replicating its weakness.

Clarity: First, to encourage private sector participation, legislation should be clear on the scope and intent of permissible information sharing and related legal protections. Section 314 implementation has suffered at times due to insufficient clarity around the scope and intent of the law. This is particularly true of Section 314(b), where the private sector has been reluctant to participate due to confusion about the types of information it may share whilst still relying on safe harbour. When setting out authorisation for public–private information sharing, governments should take steps to ensure that the scope of provisions is sufficiently clear and broad to encourage participants to undertake responsible exchanges as frequently as reasonably possible, with reassurance that they will be protected from litigation when they do so responsibly. Private sector participants need governments to provide explicit guidelines to encourage sharing and protect against litigation.

Consensus: Second, consensus between the public and private sectors about the objectives of information-sharing arrangements and related legal provisions is necessary to achieve meaningful outcomes. The public and private sectors' views on the ultimate goals and purpose of information sharing must align. Section 314’s implementation has encountered challenges where the public and private sectors have had differing views on the purpose of its provisions. Whilst a perfect harmony of views is of course unrealistic, the public and private sectors should work closely to achieve agreement on the objectives of information-sharing programmes.

Functionality: Third, legislative authorisation for information sharing should be supported by robust technical mechanisms and collaborative fora that facilitate the secure and timely exchange of information. As this study has detailed, Section 314 implementation has been hindered at times throughout its history owing to insufficient technical platforms and real-time fora for exchanging information. Merely providing legislative authorisation for information sharing is not sufficient; governments should consider how best to facilitate the sharing of information in a manner that assists the private sector in generating actionable FININT. Testing information-sharing processes and platforms via small-scale pilot programmes prior to widespread roll-out across the financial sector is also advisable for avoiding embedded inefficiencies.

Proactive Engagement: Fourth, the private sector should be trusted to identify threats with discretion, but governments, and financial intelligence units (FIUs) in particular, should be active, engaged guides that provide the private sector with timely and useful information about threats. One advantage of the US approach to public–private information sharing is that it demonstrates the public sector’s trust in the private sector: law enforcement entrusts financial institutions with sensitive law enforcement information under Section 314(a); and under Section 314(b), financial institutions are accorded significant discretion in identifying and sharing information on threats. This arrangement encourages a genuinely collaborative approach to FININT generation. Just as importantly, the US approach has seen FinCEN evolve from a largely neutral player to an active driver of FININT generation, particularly where it can point private sector FININT-gathering requirements at specific targets under Section 311.
Prioritisation: Fifth, information-sharing partnerships should balance an approach that is risk-based and directed at identifying specific high-priority threats, but sufficiently broad to capture a range of emerging threats as well. The US approach to information sharing has the benefit of allowing the public sector to direct attention at specific threats, whilst permitting the private sector to detect and report separately on a broad range of illicit financial activities. Under Section 311, FinCEN can direct the private sector to report on what it determines are the highest-priority threats to the financial system; under Section 314(a), law enforcement agencies can direct the attention of financial institutions to an even broader range of targets. Section 314(b) allows the US to cast a still broader net by permitting financial institutions to collaborate with one another before filing SARs on the wide range of threats they encounter in their day-to-day business. The result is a risk-based information-sharing system that promotes prioritisation of resource and effort.

Inclusiveness: Sixth, to counter the ability of criminals to operate swiftly across the financial sector, information-sharing arrangements should aim to involve as many types of financial institutions and law enforcement agencies active in a jurisdiction as is reasonably possible. Today’s financial sector is one that allows for large quantities of money to be sent swiftly around the globe through a variety of financial institutions, from banks to money service businesses to broker-dealers and beyond. This dynamic means that for information sharing to be relevant, it must stretch across various elements of the financial sector, and must be available to a wide range of law enforcement agencies. Doing so, however, requires having robust data protection measures in place. Determining how best to share information across international borders may be the next great challenge in this regard.

Flexibility: Finally, arrangements should be adaptable and open to amendment to keep pace with changing threat landscapes and evolving compliance challenges. The ability of new threats to emerge and place new strains on the public and private sectors requires information-sharing arrangements that are dynamic. One strength of the US approach is that it is frequently evolving. Since Section 314’s adoption, a greater range of law enforcement agencies have been brought into the fold; similarly, for all Section 314(b)’s limitations, private sector actors are collaborating to find innovative solutions for permitting information exchanges. Section 311, for its part, offers FinCEN a significant tool that it can direct at diverse and evolving threats. Governments seeking to facilitate FININT partnerships must be prepared for the likelihood that those partnerships will need to adapt almost as soon as they are put into place. Meeting this challenge requires sustained and open-minded engagement from the private and public sectors alike.
About the Author

David Carlisle is an independent consultant specialising in devising strategies for combating financial crime. He has been based in London since 2012. From 2007 to 2011, David held various roles in the US Department of the Treasury’s Office of Terrorism and Financial Intelligence, where he worked on US policy related to anti-money laundering, countering terrorist financing and economic sanctions regimes. David holds a Master’s in International Relations from the Johns Hopkins School of Advanced International Studies.